Premier Reference Source

Nuclear Power Plant Instrumentation and Control Systems for Safety and Security

Michael Yastrebenetsky and Vyacheslav Kharchenko

IGI GLOBAL
DISSEMINATOR of KNOWLEDGE

Nuclear Power Plant Instrumentation and Control Systems for Safety and Security

Michael Yastrebenetsky
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Vyacheslav Kharchenko
*National Aerospace University named after N.E. Zhukovsky KhAI,
& Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine*

A volume in the Advances in
Environmental Engineering and Green
Technologies (AEEGT) Book Series

ENGINEERING
SCIENCE REFERENCE
An Imprint of IGI Global

Managing Director:	Lindsay Johnston
Production Manager:	Jennifer Yoder
Development Editor:	Christine Smith
Acquisitions Editor:	Kayla Wolfe
Typesetter:	Christina Barkanic
Cover Design:	Jason Mull

Published in the United States of America by
Engineering Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Nuclear power plant instrumentation and control systems for safety and security / Michael Yastrebenetsky and Vyacheslav Kharchenko, editors.
pages cm
Summary: "This book evaluates the risks inherent to nuclear power and methods of preventing accidents through computer control systems and other such emerging technologies"-- Provided by publisher.
Includes bibliographical references and index.
ISBN 978-1-4666-5133-3 (hardcover) -- ISBN 978-1-4666-5134-0 (ebook) -- ISBN 978-1-4666-5136-4 (print & perpetual access) 1. Nuclear power plants--Safety measures. 2. Nuclear power plants--Instruments. 3. Digital control systems. 4. Computerized instruments. 5. Nuclear power plants--Accidents--Prevention. 6. Nuclear power plants--Ukraine--Safety measures. I. Yastrebenetsky, Michael, 1934- II. Kharchenko, Vyacheslav, 1952-
TK9152.N785 2014
621.48'35--dc23
2013046143

This book is published in the IGI Global book series Advances in Environmental Engineering and Green Technologies (AEEGT) (ISSN: 2326-9162; eISSN: 2326-9170)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series

ISSN: 2326-9162
EISSN: 2326-9170

Mission

Growing awareness and focus on environmental issues such as climate change, energy use, and loss of non-renewable resources have brought about a greater need for research that provides potential solutions to these problems. The field of environmental engineering has been brought increasingly to the forefront of scholarly research and, alongside it, environmentally-friendly, or "green," technologies as well.

Advances in Environmental Engineering & Green Technologies (AEEGT) Book Series is a mouthpiece for this research, publishing books that discuss topics within environmental engineering or that deal with the interdisciplinary field of green technologies.

Coverage

- Alternative Power Sources
- Biofilters & Biofiltration
- Contaminated Site Remediation
- Green Transportation
- Industrial Waste Management & Minimization
- Policies Involving Green Technologies & Environmental Engineering
- Pollution Management
- Renewable Energy
- Sustainable Communities
- Waste Management

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series (ISSN 2326-9162) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-environmental-engineering-green-technologies/73679. Postmaster: Send all address changes to above address. The views expressed in this series are those of the authors, but not necessarily of IGI Global.

Titles in this Series

For a list of additional titles in this series, please visit: www.igi-global.com

Nuclear Power Plant Instrumentation and Control Systems for Safety and Security
Michael Yastrebenetsky (State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine) and Vyacheslav Kharchenko (National Aerospace University- KhAI, Ukraine, and Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine)
Engineering Science Reference • copyright 2014 • 364pp • H/C (ISBN: 9781466651333) • US $235.00 (our price)

Computational Intelligence in Remanufacturing
Bo Xing (University of Pretoria, South Africa) and Wen-Jing Gao (Meiyuan Mould Design and Manufacturing Co., Ltd, China)
Information Science Reference • copyright 2014 • 348pp • H/C (ISBN: 9781466649088) • US $195.00 (our price)

Risk Analysis for Prevention of Hazardous Situations in Petroleum and Natural Gas Engineering
Davorin Matanovic (University of Zagreb, Croatia) Nediljka Gaurina-Medjimurec (University of Zagreb, Croatia) and Katarina Simon (University of Zagreb, Croatia)
Engineering Science Reference • copyright 2014 • 433pp • H/C (ISBN: 9781466647770) • US $185.00 (our price)

Marine Technology and Sustainable Development Green Innovations
Oladokun Sulaiman Olanrewaju (University Malaysia Terengganu, Malaysia) Abdul Hamid Saharuddin (University Malaysia Terengganu, Malaysia) Ab Saman Ab Kader (Universiti Teknologi Malaysia, Malaysia) and Wan Mohd Norsani Wan Nik (University Malaysia Terengganu, Malaysia)
Information Science Reference • copyright 2014 • 338pp • H/C (ISBN: 9781466643178) • US $195.00 (our price)

Sustainable Technologies, Policies, and Constraints in the Green Economy
Andrei Jean-Vasile (Petroleum and Gas University of Ploiesti, Romania) Turek Rahoveanu Adrian (Institute of Research for Agricultural Economics and Rural Development, Romania) Jonel Subic (Institute of Agricultural Economics, Belgrade, Serbia) and Dorel Dusmanescu (Petroleum and Gas University of Ploiesti, Romania)
Information Science Reference • copyright 2013 • 390pp • H/C (ISBN: 9781466640986) • US $180.00 (our price)

Energy-Aware Systems and Networking for Sustainable Initiatives
Naima Kaabouch (University of North Dakota, USA) and Wen-Chen Hu (University of North Dakota, USA)
Information Science Reference • copyright 2012 • 469pp • H/C (ISBN: 9781466618428) • US $180.00 (our price)

Green and Ecological Technologies for Urban Planning Creating Smart Cities
Ozge Yalciner Ercoskun (Gazi University, Turkey)
Information Science Reference • copyright 2012 • 404pp • H/C (ISBN: 9781613504536) • US $180.00 (our price)

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE
www.igi-global.com
701 E. Chocolate Ave., Hershey, PA 17033
Order online at www.igi-global.com or call 717-533-8845 x100
To place a standing order for titles released in this series, contact: cust@igi-global.com
Mon-Fri 8:00 am - 5:00 pm (est) or fax 24 hours a day 717-533-8661

Editorial Advisory Board

List of Reviewers

Table of Contents

Detailed Table of Contents

Operation reliability of NPP I&C and its components is considered in this chapter. Besides quantitative measures, qualitative features that provide required functional reliability such as protection against Common Cause Failures (CCF), single-failure criterion, redundancy, diversity, prevention of personnel errors, and technical diagnostics, are discussed. A group of features of NPP I&C and its components, united by "performance resistance," is also considered. In particular, they are resistance to environment influences, mechanical influences (including earthquake impacts), insensitivity changes of power supply, and electromagnetic disturbances. Operation quality issues are considered. By quality (in a broad sense), the authors mean the accuracy, response rate characteristics, and features of human-machine interfaces. Features that provide NPP I&C independence from malfunction or removal from operation of system components (including redundant ones) or from adjacent NPP I&C, and the decrease of possible impact of components on other adjacent systems (electromagnetic emission, fire safety) are described as well.

FPGA is a convenient technology that is being applied intensively to build I&CS for critical industries like NPPs. Practical experience confirms that in some cases application of the FPGA technology is much more reasonable than application of other technologies like microprocessors, etc. Experience of RPC Radiy in FPGA-based I&C development is provided in this chapter, as well as general information on FPGAs. Dependability of NPP I&CS is an important but challenging task. There are several techniques that can be applied for safety and dependability assessments, but all of them have limitations and cannot be easily applied in most cases. Sometimes combined usage of different methods is the most appropriate solution. Techniques of dependability assessment and achievement developed and used by RPC Radiy, as well as elements of the assessment methodology are briefly described.

Features of software as a component of Instrumentation and Control (I&C) systems are analyzed. Attention is paid to the importance of functions performed by software and hazards of such software. Requirements for characteristics of software as a component of I&C systems are analyzed. Different regulatory documents are considered in order to disclose common approaches to the use of dedicated software and off-the-shelf software components. Classification of software, as well as classification of requirements, is described. Criteria of selection and structuring of requirements, as well as criteria for software verification, are defined. As long as the characteristics of software components directly depend on the quality of the processes of software development and verification, requirements for software life cycle processes are considered. The second part of this chapter is dedicated to evaluation of software for nuclear power plant I&C system. Criteria and principles of evaluation are observed. Evaluation of the characteristic of software as a product and software development and verification processes are considered.

Chapter 8 considers design principles of Overall Instrumentation and Control (OI&C) systems implemented at Ukrainian NPPs. The first section provides brief information on controlled objects—power units with reactors WWER, which are operated at Ukrainian NPPs. The main principles and features for modernization of OI&C systems and their components in NPPs in Ukraine that were generated in 2000-2011 are further provided. The third section is dedicated to the architecture of OI&C systems that control technological processes on these power units. After that, the central part of this architecture, a group of the most closely connected individual Instrumentation and Control (further, I&C) systems, for which the general term “reactor control and protection system” is used in Ukraine and Russia, is considered in detail. The purpose, composition, and structure of a modernized reactor control and protection system that are implemented at Ukrainian NPPs with WWER reactors are provided.

In Chapter 9, Emergency and Preventive Reactor Protection (E&PRP) systems implemented at the Ukrainian NPPs during 2003-2013 are considered. The core of E&PRP systems is formed by software-hardware complexes (SHC E&PRP) developed on the base of the Research and Production Corporation “Radiy” equipment family. The first part describes the main purposes of E&PRP: forced power reduction or immediate reactor shutdown to prevent an emergency from developing into an accident. The second part describes the basic functions determined by the system purposes, along with additional functions performed by SHC E&PRP. The third part is devoted to describe SHC E&PRP technical characteristics, which implement the specified functions. The forth part deals with information about the composition and structure of SHC E&PRP, as well as about connections of SHC E&PRP with adjacent I & C systems are shown. In the fifth part, aspects of functional safety assurance during development, production, and acceptance of SHC E&PRP are considered.

Chapter 10 considers the Rod Group and Individual Control (RG&IC) system, which is one of the individual I&C systems and a part of the reactor control and protection system. RG&IC is an actuation system, which performs functions initiated by emergency and preventive reactor protection, reactor power control, unloading, limitation and accelerated preventive protection, and remote control rod position commands sent by the power unit personnel. The central part of RG&IC system consists of software-hardware complex SHC RG&IC-R based on the equipment family of the Research and Production Corporation “Radiy” (RADIY PLATFORM – see Chapter 1). The RG&IC system combines functions that belong to A and B categories according to safety impact (IEC, 2009), relates to safety class 2(A) and complies with the fundamental safety principles (IAEA, 1999), requirements that are set forth in international standards (IAEA, 2002, 2012; IEC, 2011), and Ukrainian nuclear safety rules and regulations (NP, 2000, 2008a, 2008b).

The chapter contains a description of Safety Parameters Display Systems (SPDS) implemented at NPP units WWER-1000 of Ukraine. These systems were designed by Westinghouse Electric Corporation (USA). LLC "Westron" (Ukraine) took development and implementation of these systems. These systems were provided at 11 NPP units in the framework of the International Nuclear Safety Program with the support of DOE (USA). The general purpose of SPDS is to provide support for operators, when abnormality of NPP unit operational conditions must be determined rapidly. The chapter considers the purpose and the functions of these systems, specific features of the displaying information about the state of the functions, which are critical for NPP unit safety, and the structure of systems. Implementation of SPDS project at 11 units of Ukrainian NPPs is a good example of USA and Ukraine collaboration in the nuclear area. Organization of this large-scale modernization is described.

Safety assessment of Instrumentation and Control systems (I&C systems) of NPP is performed during expert reviews of nuclear and radiation safety in the framework of the licensing process at all life cycle stages of I&C systems. Life cycle stages of NPP I&C systems, which are determined by current guides, rules, and standards of Ukraine, are considered in the chapter. A short overview of the main principles of safety regulation of nuclear facilities, licensing, and expert review of nuclear and radiation safety is presented. Specific safety assessments of NPP I&C systems at different life cycle stages are analyzed (in particular, a list of documents proving NPP I&C safety that should be submitted for expert review at each stage is given). Such assessment is a labor-intensive process that requires processing considerable amounts of a variety of information. Hence, it is reasonable to provide experts with information support for assessing the safety of NPP I&C systems. The chapter gives suggestions and examples of practical implementation of the automated system for support of expert activities and considers the knowledge base for I&C systems.

The problem of the safe interaction between a Nuclear Power Plant (NPP) and a Power Grid (PG), considering the Fukushima nuclear accident, is becoming topical. There are a lot different types of influences between NPPs and PG, which stipulate NPPs' safety levels. To evaluate the influences, two metrics are proposed: linguistic and numerical. The approach to the NPP-PG safety assessment is based on the application of Bayesian Belief Network (BBN), where nodes represent different PG systems and links are

Preface

It is difficult to overestimate the importance of safety problems at Nuclear Power Plants (NPP) for all countries in which they operate. This issue is extremely important in the context of energy safety and of the safety of mankind as a whole. Unfortunately, the accident at Fukushima-1 NPP (2011), which extended the list of major nuclear power plant accidents including Three Mile Island (1979) and Chernobyl NPP (1986), confirmed this conclusion.

Instrumentation and Control (I&C) systems, which create conditions to prevent incidents in NPP operation and mitigate the accident consequences, play a big role in NPP safety assurance.

In past decades, the main technological process of electric power production at operating NPPs has not undergone significant changes. However, in recent years, significant changes have been made in the design of I&C systems. At first, the digital technology in NPPs was widely applied for performing information functions in contrast to control functions. However, after the accumulation of essential experience in the design of computer control systems for critical safety objects and in justification that such systems meet safety requirements, intensive implementation of computer systems for control and protection of nuclear reactors has begun.

In the recent years, the development of modern information technologies and achievements in the field of electronics have allowed for the improvement of functional capabilities and I&C systems reliability. These facts have led to obsolescence of previously installed I&C systems at operating NPPs, which, along with physical aging of equipment, necessitated the modernization of a considerable number of I&C systems.

Significant toughening of requirements for NPP safety has led to the modification of international and national standard bases related to NPPs as a whole. This fact, together with the use of modern information and electronic technologies (such as Field Program Gate Array – FPGA), has also caused the necessity to revise international standards for I&C systems, determined, first of all, by documents of the International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC).

For example, IAEA standards related to NPP I&C systems were issued in 1980 (IAEA, 1980) and 1984 (IAEA, 1984), updated in 2002 (IAEA, 2002) and again in 2011-2013 (IAEA, 2013).

According to international and national regulatory documents, all NPP I&C systems (as well as other systems) are classified depending on their safety impacts. Methodology of their differentiation is distinct in different countries, but the concept of system differentiation by safety impacts is conventional.

This book focuses on NPP I&C systems relevant to safety and named “safety important systems” according to the IAEA classification and classification of a range of countries. The examples of such systems are the reactor trip system, refueling machine control system, reactor power regulation and limitation system, etc. Safety important systems play a crucial role in the control and monitoring of NPP operation; they also detect conditions in which power unit operation becomes unsafe and, if necessary, shut the reactor down.

Safety important NPP I&C systems have a set of different peculiarities: the necessity of ensuring high operating reliability and of meeting a set of requirements essential in the safety context. For all NPP safety important systems, including I&C systems, the presence of a national regulatory body—government organization, independent from NPP, designers, and manufactures of I&C systems and equipment—is very important. The names of these organizations are different in various countries (e.g. U.S. Nuclear Regulatory Commission in the USA, State Nuclear Regulatory Inspectorate in Ukraine). According of the Convention on Nuclear Safety (IAEA, 1994), which is approved by all countries operating NPPs, the main tasks of the regulatory body are to establish:

Applicable national safety requirements and regulations (including requirements on I&C systems).

- A system of licensing with regard to nuclear installations and the prohibition of the operation of a nuclear installation without a license (including licensing related to installation of I&C systems).
- A system of regulatory inspection and assessment of nuclear installations to ascertain compliance with applicable regulations and the terms of licenses (including inspection and assessment of operating NPP I&C systems).

High functional reliability is required not only for NPP I&C systems but for I&C systems in many other applications, where the safety problem is an essential one. Examples are I&C systems for chemical and petrochemical industries, for many types of transport such as air transport, sea transport, rail transport (especially high-speed transport), and for some types of medical equipment, etc.

In recent years, such systems have been called critical safety systems or safety-related systems. Let us mention that concepts of safety assurance of critical I&C systems in different branches of activities have considerably fewer differences than concepts of equipment safety controlled by these systems. For example, the comparison of safety concepts for the NPP unit control system and for a dangerous weapon, such as a missile career with nuclear warheads, displayed the considerable community of such concepts with all the variety of controlled objects (Aizenberg, 2002).

Safety is a predominant attribute of NPP I&C. Other attributes such as reliability, maintainability, availability, and security are “slave” to safety. In a set of these attributes, it is necessary to mark out security and integrity as its most important component. Due to the fast evolution of methods and technologies of unauthorized information intrusions, the set of vulnerabilities of I&C, and their components, as well as attention to the development of regulatory requirements on NPP I&C security, methods, and means of its analysis and assurance, have increased significantly. This fact determines a necessity to consider answers for challenges in this field in the context of general problems of NPP I&C safety.

The book is written by authors from Ukraine: staff of the State Scientific and Technical Centre for Nuclear and Radiation Safety (SSTC NRS), a technical support organization of the Ukrainian Regulatory body; Research and Production Corporation Radiy, the biggest Ukrainian company developing, manufacturing and implementing NPP I&C; Scientific Technical Centre for Safety Infrastructure-Oriented Research and Analysis; and the “Computer Systems and Networks Department” of National Aerospace University, or KhAI. The book summarizes the experience of Ukrainian specialists. This experience is of interest due to the following reasons:

First, Ukraine has undergone a severe accident at the Chernobyl NPP. This had a significant impact on the evolution of nuclear power engineering in Ukraine, including the progress of NPP I&C. The lessons of this accident have significantly contributed to the solution of numerous issues connected with NPP safety assurance in Ukraine: improvement of NPP operation culture, improvement of NPP equipment quality (including I&C systems, which are considered in the book), and application of more stringent safety requirements (including requirements on I&C). Qualitative changes were made in governmental safety regulation. Therefore, specialists who directly participated in the mitigation of this accident's consequences came to operators, to the Ukrainian regulatory body, and to SSTC NRS. The experiences of these people were invaluable and were transferred from this generation to the next one.

Second, Ukraine is a pioneer in wide application of Field Programmable Gate Arrays (FPGA) in safety important NPP I&Cs. Nowadays, reactor protection systems, engineering safety feature actuation systems, and others were designed at the Research and Production Corporation Radiy and successfully operated in NPPs. These systems are applied not only in NPPs in Ukraine, but also in other countries. The main advantages of these systems are high reliability and safety, confirmed by 10 years of application experience, relative simplicity and "clarity" in verification of control safety functions, equipment compactness, and short terms of I&C systems replacement during modernization.

Third, Ukraine has experience in complete modernization of nearly all NPP I&C systems by new modern computer systems, performed at all 15 power units within the past years.

ORGANIZATION OF THE BOOK

The book is organized into 13 chapters. A brief description of each chapter follows.

Chapter 1 contains definitions of the main terms in this book—Instrumentation and Control (I&C) system, individual and overall I&C system, Software-Hardware Complex (SHC), etc. Boundaries of I&C systems and their typical parts are described. General information about I&C systems, based on the use of up-to-date digital methods, is provided. The main peculiarities of such systems, which are described in more detail in further chapters of this book, are considered.

Chapter 2 describes the main standard bases for NPP I&C systems—documents of the International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC). Classifications of I&C systems and their components are given on the basis of their safety impact. All systems are divided into safety important and non-safety important. Thus, safety important systems can be safety systems and safety related systems. According to IEC, functions to be performed by I&C systems shall be assigned to categories according to their importance to safety. A comparison of different types of classification of I&C systems is shown.

Chapter 3 provides the main properties of safety important NPP I&C. These properties are divided into groups related to functional reliability (redundancy, single-failure criterion, protection against common cause failures, etc.), resistance (resistance to environmental impacts, mechanical impacts, seismic impacts, electromagnetic compatibility, change of power supply parameters), operation quality (accuracy, time characteristics, human-machine interface), and independence of functions performed.

Chapter 4 describes the element base of the new generation of NPP I&C, namely Field Programmable Gate Array (FPGA). The peculiarities of FPGA application to the design of safety critical systems is also discussed. FPGA chips are modern complex electronic components which are applied in NPP I&C during the last 10-12 years. The advantages and some risks caused by the application of FPGA technology are analyzed. Safety assessment techniques of FPGA-based I&C systems and experience of their creation are described as well.

Chapter 5 contains classification and description of requirements on safety important NPP I&C software (SW). SW peculiarities as an object of safety assessment are analyzed. The facts illustrating the increase of SW faults' influence on reliability and safety as NPP I&C and computer-based systems for different critical applications are discussed. The criteria applied to assess SW are described. The methods and tools for evaluation of SW reliability and safety are analyzed.

Chapter 6 analyzes in detail the diversity as one of the main principles of NPP I&C safety assurance. The taxonomy of multi-version computing applied to I&C is formulated. Classification schemes and different types of diversity for SW- and FPGA-based I&C are analyzed. Methods and tools for support of assessment and safety assurance of multi-version I&C are described. The tasks related to the choosing of diversity types on development of multi-version I&C are formulated and solved, taking into account sets of cost and diversity metrics.

Chapter 7 is devoted to the description of the security problem applied to NPP I&C. Challenges in this field, taking into account element base including FPGA and SW components of NPP I&C, are discussed. Three groups of international and national standards containing the requirements on NPP I&C security assessment and assurance and on application of complex electronic components, particularly FPGA, in critical domains are analyzed to define a set of the requirements on FPGA-based NPP I&C security. The method of security assessment based on techniques in Gap and IMECA analysis is described. The ways of security improvement using different countermeasures are proposed.

Chapter 8 contains brief information on controlled object-units with WWER reactors operated in Ukraine, on the overall I&C system for these units, and on main principles and features of big-scale modernization of overall I&C system and their components, which were performed in Ukraine during 2000-2012 years. Architecture and functions of overall system and the main individual systems included in overall system are described.

Chapters 9-10 give a description of individual systems with FPGA application for power units with WWER reactors: reactor protection systems (emergency and preventive protection) and reactor control rod systems. The core of these systems is formed by software-hardware complexes, developed on the basis of the equipment family of Research and Production Corporation Raidy. Every chapter contains the main purposes of systems, the basic functions determined by the systems purposes, technical characteristics, composition and structure of software-hardware complexes, its components, connections with peripheral equipment and adjacent I&C-systems, and aspects of functional safety assurance.

Chapter 11 considers Safety Parameters Display Systems (SPDS), which were designed in the USA (Westinghouse Electric Corporation) and applied at 11 power units with WWER-1000 reactors on Ukrainian NPPs. Implementation of SPDS is a good example of collaboration between the USA and Ukraine. A lot of different problems were solved for the implementation: a large number of systems are being introduced; the lack of normative documents that are in effect in Ukraine, which contain requirements for SPDS; differences in safety classification and in general normative requirements for safety in Ukraine and in the USA.

Chapter 12 contains a description of the overall safety life cycle of I&C systems and components. The main principles of the NPP I&C safety assessment used in Ukraine are described. This assessment was fulfilled by the technical support organization in the frame of expert reviews of documents that substantiated the NPP I&C functional safety. The knowledge base on NPP I&C for the information support of the expert review process is described.

Chapter 13 is devoted to the analysis of interconnection and interaction of NPPs and power grid with a reliability and safety point of view. Operation disturbances in power grid consisting of different systems including NPP, caused by natural disasters, failures, human factors, terrorism, and so on, are systemized. Approaches and techniques, which allow for evaluation of the mutual influences between NPP and power grid, understanding the dynamic risks caused by their interactions, are researched. The proposed infrastructure safety assessment techniques are considered an essential part of power grid risk management and decision-making system. They allow for the avoidance of disturbances or for the minimization of their consequences during the interaction of NPP and power grid.

The book is intended for specialists involved in:

- Development and manufacture of components for safety important I&C.
- Design and operation of safety important NPP I&C systems.
- Licensing of NPP I&C systems and their components.

The book may also be useful for specialists who participate in the development and operation of safety control I&C systems (e.g., in airspace, railway, chemical industry, etc.). Experience in safety important functions performed with FPGA may be of interest to specialists from different branches that use these elements.

The book may also be of interest to students and lecturers at universities in specialties related to computer and software engineering and its critical applications and to nuclear engineering.

Michael Yastrebenetsky
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Vyacheslav Kharchenko
National Aerospace University named after N.E. Zhukovsky KhAI, Ukraine & Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

REFERENCES

Aizenberg, Y., & Yastrebenetsky, M. (2002). Comparison of safety assurance principle of control systems for missile careers and nuclear power plants. *Cosmic Science and Technics, 1*.

IAEA. (1980). 50-SG-D3. *Protection system and related features in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1984). 50-SG-D8. *Safety-related instrumentation and control systems for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1994). *Convention on nuclear safety*. Vienna, Austria: IAEA.

IAEA. (2002). NS-G-1.3. *Instrumentation and control systems important to safety in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (2013). DS-431 (Draft). *Design of instrumentation and control systems for nuclear power plants*. Vienna, Austria: IAEA.

Kharchenko, V. (Ed.). (2011). Safety of critical infrastructures: Mathematical and engineering methods. Kharkiv, Ukraine: National Aerospace University KhAI.

Acknowledgment

The authors thanks colleagues of the State Scientific and Technical Centre for Nuclear and Radiation Safety, Research and Production Corporation Radiy, Scientific Technical Centre for Safety Infrastructure-Oriented Research and Analysis, "Computer Systems and Networks Department" of National Aerospace University KhAI for their attention to work.

Colleagues of the State Scientific and Technical Centre for Nuclear and Radiation Safety, V. Filon, Y. Malinovska, S. Koroleva, and S. Trubchaninov, and colleagues of the Scientific Technical Centre for Safety Infrastructure-Oriented Research and Analysis, A. Kashina and L. Kharchenko, assisted in the preparation of the manuscript for publication.

Colleagues of the "Computer Systems and Networks Department" of National Aerospace University KhAI participated in discussions of a lot of problems considered in the book. They concerned application of FPGA in NPP I&C and other critical domains, software safety assessment, security analysis, research, development, and implementation of multi-version systems. In addition, the authors thank to participants of the standing seminar "Critical Computer Systems and Networks" who worked at the department for 12 years.

Contacts with the IAEA Technical Working Group on Nuclear Power Plant Instrumentation and Control (scientific secretaries during last years – K-S. Kang, O. Glockler, J. Eiler) and with the International Electrotechnical Commission Technical Committee TC 45 "Nuclear Instrumentation" Subcommittee SC 45A "Instrumentation and Control of Nuclear Facilities" (Chairman – G. Johnson) offered the possibility to attend a course on the modern state of work related to NPP I&C systems.

The authors and editors express a special thankfulness to reviewers of the chapters, who represent universities and research centers from Italy, Russia, Slovak Republic, Ukraine, and USA.

The remarks and recommendations of the reviewers were very helpful and improved quality of the presented chapters.

The authors are thankful in advance for critical reviews and suggestions, which further will be taken into account during design, analysis, and assurance of NPP I&C safety.

Michael Yastrebenetsky
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Vyacheslav Kharchenko
National Aerospace University named after N.E. Zhukovsky KhAI, Ukraine & Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Chapter 1
General Provisions

Michael Yastrebenetsky
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Yuri Rozen
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

ABSTRACT

This chapter contains definitions of the main terms in this book—Instrumentation and Control (I&C) system, individual and overall I&C system, central part of the I&C system and peripheral equipment, Software-Hardware Complex (SHC), Commercial Of The Shelf (COTS) products, and equipment family (platforms). Differences between the SHC and I&C system are explained. General information about I&C systems, based on the use of up-to-date digital methods and facilities of obtaining, transferring, processing, and displaying of data, is provided. The main peculiarities of such systems, which are described in more detail in further chapters of this book and illustrated by the given examples of implementation of specific systems, are considered.

INTRODUCTION

I&C systems play a significant role in assurance of safety and security of nuclear power plants (NPP). These systems perform automatic control of technological processes and equipment in operational modes; support operating personnel that monitor equipment condition and/or control processes; take part in performance of functions related to prevention of nuclear accidents, which could harm the population, personnel, environment and NPP itself; archive, display and record data required for analysis of causes, progression of accident and recovery of safe controlled mode at NPP. In this connection, the role of I&C systems is steadily increasing, while improvement of digital technology, new complex electronic components, including Field Programmable Gate Arrays (FPGA), distributed architecture of the I&C with local computer nets for exchange of information, use of optoelectronic channels of communications, etc.

The object of the chapter is to explain basic notions required for better understanding of further chapters of the book to readers.

BACKGROUND

Formation of a new scientific and technical trend is nearly always followed with discussions, occurred due to initial uncertainty of used terminology. I&C systems intended for nuclear power plants are not an exception. There are several glossaries

DOI: 10.4018/978-1-4666-5133-3.ch001

related to this trend, in particular: Rosenberg & Bobryakov, 2003; IAEA, 2007,a developed by International Atomic Energy Agency (IAEA); IEC, 2007, developed by the International Electrotechnical Commission (IEC). In the book IAEA, 2011, prepared by an international group of specialists under the auspices of the IAEA, general concepts applicable to NPP I&C systems, and introductory description of I&C systems and their life cycle are considered. Moreover, in many international and national regulatory documents related to individual tasks of design and/or operation of NPP I&C systems definitions of used terms are provided.

However, the terminology regulated in Ukrainian regulations, rules and standards can be unknown to readers of the book, so in the first chapter some terms, used in other chapters, are defined and supplied with annotations. In particular, the concept of "Instrumentation and control systems" that is traditionally used in Ukraine in narrower sense than in international standards and English literature, where this term, depending on context, can cover not only individual I&C systems, but also the overall set of such systems, controlling a certain object or, by contrast, only central part of individual I&C system and also equipment (hardware, integrated with software), developed and/or produced and supplied for implementation of the central part of individual I&C systems, is considered. For such equipment the authors use the term "Software-hardware complex" (SHC) that does not have an analogue in international standards, but is widely used by Ukrainian experts, and it is embodied in Ukrainian national standards (and some other countries) and in literature, for example, in Yastrebenetsky, 2004.

This fact necessitates detailed consideration of the concept, denoted by the term SHC, peculiarities that distinguish it from the individual I&C system, and differences between SHCs as industrial production products, in the first chapter.

Software of modern distributed overall I&C systems significantly differs from the one that was used in centralized systems of previous generation: it is concentrated mainly in SHC and integrated with hardware directly at the plant that design, manufactures and and/or supplies Software-hardware complex, but not at the facility (NPP), where the system will be operated. These and other differences important for understanding of further book content are also considered in the chapter.

From the beginning of creation and use of software-hardware complexes in Ukraine intended for individual I&C systems, a principle of assembling (aggregation) such SHC from a limited set of parts (hardware, software), composing an aggregate equipment family, oriented at solving I&C tasks typical for a sufficiently wide range of objects in one or several branches of industry, was applied. As far as all I&C systems, described in the book, are designed on the basis of such equipment families (platforms), general information about these platforms and also those similar equipment families, developed in other countries, are provided

In the chapter at the beginning of the book, the authors decided to describe their vision of development trends of I&C systems, which are implemented in practice in the modernization of current and designing of new systems for Ukrainian NPPs.

Recent years are characterized by rapid development of electronics, digital computer technologies, information technologies, which are more widely used in the process of design of I&C systems. Advantages of these systems are the following:

- Increase of operating speed and storage capacity allowing on-line complex calculations in real time, required for implementation of control and security algorithms.

- High reliability of component parts (electronic components and computer technology), having a crucial influence on the reliability of devices and systems based on them, which can be applied for solving more responsible tasks related to safety assurance.
- A high degree of integration of applied electronic components, which allows a significant decrease in the number of components and use simple connections between them, that also facilitate the increase of reliability while the requirements on functionality are complied with (or even amplified).
- Continuous decrease of the relative value of component parts allows significantly improvement of functional capabilities and characteristics of designed systems, without exceeding the limits of accepted costs.
- One of the results is a possibility of wider use of redundancy, including structures with multiple redundancy, performing logic conditions "two-out-of-three," "two-out-of-four," etc., which were earlier used only in the most responsible cases.
- Simplicity of software modification determines the required flexibility of I&C systems, allowing adapt of one and the same hardware for solving different tasks of control and management by means of software, development of functional capabilities, change of system characteristics in the process of operation, etc.
- Adoption of high quality means of manual input and display of information (wide-screen liquid-crystal monitors with high resolution, touch panels, keyboards, manipulators, etc.) and software developed for them allow implementing "friendly" human-machine interfaces, comparable by functionality and usability with those that have already become common for up-to-date computers, in I&C systems.
- Use of local computer networks and relevant network equipment for data exchange between devices included in individual I&C system and also between component parts of the overall I&C systems promotes significant saving of cable products, decreases labor expenditures of mounting, adjustment and maintenance, allows a high speed of transfer and required reliability of messages with their transfer over fiber-optic lines, as well as required noise immunity of transfer in the electromagnetic environment typical for industrial facilities.
- Nearly unlimited possibilities of up-to-date computer technology for long-term storage of large scope of information are also topical for I&C systems, which in the process of operation allow performing continuous archiving of current data that can be requested and used to determine cause of emergencies, analysis of the sequence of events, assessment of actions of mechanical systems and personnel, accident management and restoration of the controlled condition, elaboration of measures for improvement of NPP safety.
- Use of built-in hardware and software, providing technical diagnostics, display and record of diagnostic messages, allows quickly detecting faults, automatically defining their locations and planning required actions for recovery of operation. This is especially important for &C systems, that perform real time control, as a delay in the process of recovery may not only cause economic losses, but also affect NPP safety.

In the process of design of I&C systems for NPP specified capabilities of modern information technologies and available for use of element base allowed:

- Use of more reliable and saving digital logic circuits instead of logic circuits based on contact-relay elements.
- Use of more accurate digital calculations, implemented by universal software controlled computer technology (microprocessors, single chip microcomputers, etc.), by complex programmable electronic components instead of analog computing circuits.
- Replacing analog measuring and control devices by digital ones with improved algorithms able to take consider specific characteristics of controlled technological equipment.
- Operating personnel to manage manually elements of technological equipment directly with keyboard workstations.
- Replacing analog recording and indicating devices on consoles and control boards, main and emergency control rooms by more reliable, accurate and ergonomic digital devices of data display and recording, including LCD monitors, panel computers, laser printers, etc.
- Implementing software-hardware peripheral equipment (sensors, actuators) with "microprocessor intellect," in which specific functions (adjustment of measurement ranges, automatic diagnostics, calibrations, etc.) are performed under control of programs stored in their read-only memory.
- Equipping every I&C system with inbuilt means of technical diagnostics, which provide continuous automatic monitoring of system and their components state (including software self-control) with a depth of fault search to one removable component part.
- Implementing distributed control of technological processes and NPP equipment, using local computer networks and fiber-optic communication lines for message exchange between geographically distributed individual I&C systems and/or component parts of these systems.

INSTRUMENTATION AND CONTROL (I&C) SYSTEMS

All systems and equipment of nuclear power plants can be divided into two categories:

- Technological systems and equipment, providing transportation, storage, processing of materials, generation and transformation of energy, protecting nuclear fuel, equipment, piping from damage and from spread of radioactive substances and ionizing radiation over the specified boundaries.
- Instrumentation and control (I&C) systems, implementing information technologies, related to obtaining of input signals from technological systems and equipment and teams of operating personnel, transfer, storage, processing of obtained information and output of control impacts on technological systems and equipment at NPP.

In IEC, 2008, regulating functional safety in different technology branches (including nuclear power engineering), a general concept "electrical /electronic/programmable electronic system," defined as "system for control, protection or monitoring based on one or more electrical/electronic/programmable electronic (E / E / PE) devices, including all elements of the system such as power supplies, sensors and other input devices data highways and other communication paths, and actuators and other output devices," is used. These systems have to interact with wide classes of equipment under control (equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activity). (See comments of the authors on the standard in the book Smith & Simpson, 2001. Among other books devoted to critical systems for control, protection or monitoring in different industry branches, Cluley, 1994 and Storey, 1996 can be mentioned.

IEC, 2011, providing a detail description of general requirements on functional safety applicable to NPPs, instead of the term E / E / PE systems introduces a more common term in industrial automatics - I&C systems, defining them as "system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself." In turn, the term I&C function is defined as "function to control, operate and/or monitor a defined part of the process."

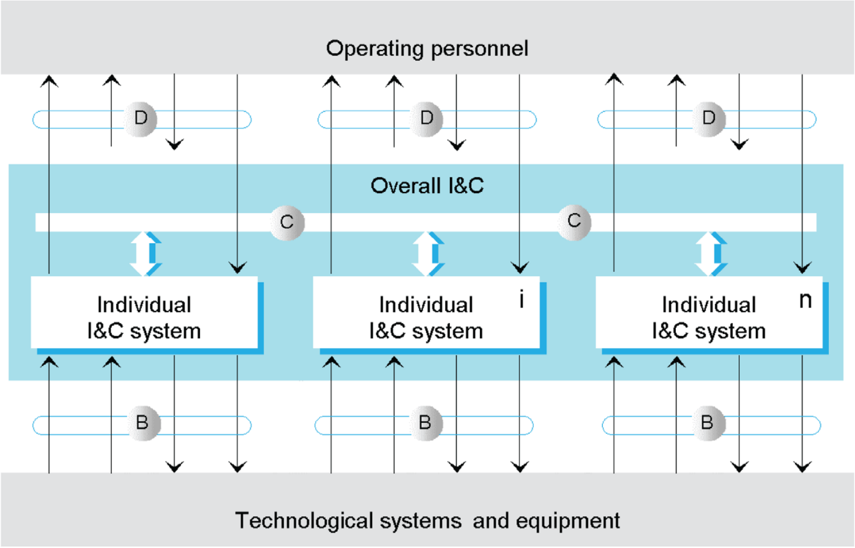
The general concept of "instrumentation and control system" covers:

- Overall I&C systems, providing monitoring and control of all technological systems and equipment at the NPP or an individual NPP unit.
- Individual I&C systems, together performing all I&C functions provided for overall I&C system, interacting with each other, with operating personnel and technological systems and equipment.

Each individual I&C system participates in one or several I&C functions, being operational autonomous, reasonably separate, and can be considered in the process of design, packaging, assembling, adjustment, testing and operation individually and independently from other component parts of the overall I&C system, in which it is contained (Figure 1).

Based on functional characteristic, individual I&C systems can be divided into:

Figure 1. Overall I&C system



B - interface with technological systems and equipment
C - interface with individual I&C system
D - human-machine interface

- *Information Systems (Figure 2 a):* Intended for obtaining, processing, storage, transfer, display and / or recording of information about the state and / or operation of technological systems and equipment or other I&C systems (performance of information functions).
- *Control Systems (Figure 2 b):* Intended for influencing the state and / or operation of technological system, equipment or other I&C systems (performance of control functions).

For example, in-core reactor monitoring system, neutron flux monitoring system, computer information system, and safety parameters display system can be related to information systems,. Examples of control systems are reactor protection system, reactor power control system, reactor group and individual control rod system, etc.

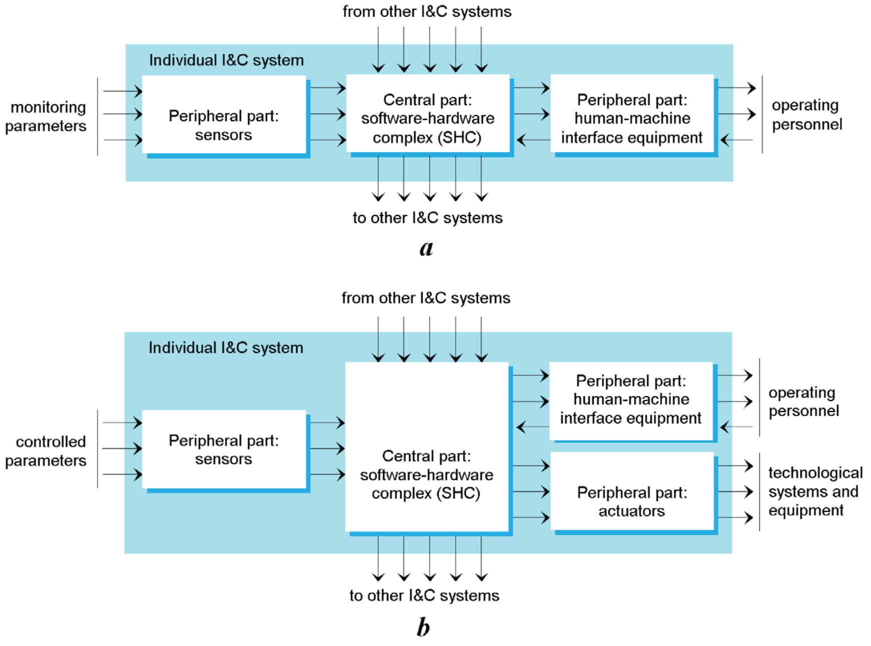
However, it should be noted that this identification is not typical for modern I&C systems: in many cases information and control functions can be combined in one system. For example, reactor power control system, along with performance of control functions provides personnel with information on controlled parameters, state of technological equipment, provided control commands, i.e. it also performs information functions. On the other hand, In-core reactor monitoring system performs information functions as well as individual control functions (for example, generating commands, initiating actuation of preventive protection if local energy release is above the acceptable rate).

Each individual I&C system is intended for performance of specific set of the main and auxiliary functions. The main functions of a system are determined by its designation:

Main *information functions* of I&C systems are monitoring, display, alarm, recording and archiving.

Monitoring functions provide reception of current data of values of technological parameters, external and internal effects, state of structures,

Figure 2. Structural schemas of individual I&C systems



a

b

systems and elements, initiating events, commands of I&C systems and operating personnel in all operating modes of the power unit and also in accidents in the mitigation of their effects (post -accident monitoring). These data can include, for example, neutron flux density, temperature, pressure and activity of the primary coolant, water level in steam generators and pressurizer, temperature, pressure and air composition under the containment and other parameters that are determined by direct measurement. The values of parameters such as the rate of neutron flux increase, burnup margin, heat power, saturated steam temperature, etc., are determined by indirect measurements (basis of basic physical dependencies that relate them to measured values of other parameters).

Display functions provide visualization of current and archival data necessary for operating personnel for monitoring of processes, operation of I&C systems and results of their own actions in the process of power unit operation in operation modes, failure of normal operation and emergency. Display of post-accident monitoring data provides NPP personnel and involved safety experts who control emergencies and mitigate their effects, with required information on the origin and progression of the accident, state of structure, systems and elements of the power unit during and after design basis and beyond design basis accidents.

Alarm functions provide visual and / or audio alarms to attraction of personnel attention to:

- Initiating event, which can cause an emergency, failures of design specific conditions for safety operation, external and internal risks (fire, earthquake, etc.), deviation of controlled parameters from their emergency alarm set-points, unavailability of technological or I&C systems for participation in performance of the required safety function (visual and audio emergency alarm).
- Failures of design specific operating limits and conditions, deviation of controlled parameters from their preventive alarm set-points, unavailability of technological or I&C systems for participation in performance of the required safety functions (visual and, perhaps, audio preventive alarm).
- Actuation of automatic protection and interlocking, switching of operating modes, energizing or de-energizing, change of set-points, unavailability of technological or I&C systems for participation in performance of functions, not important to safety (visual indicator alarm).

Recording functions provide preparation of data and automatically printing of documents in specified format on paper carriers (on schedule or in case of predetermined events) and / or on call of personnel, continuous recording of graphs showing variation of individual controlled parameters and / or groups of interconnected parameters with time.

Archiving functions provide memorization of monitoring data in chronological order and storage of obtained data within a specified time period in the process of power unit operation in operating modes, failures of normal operation, in emergencies, accidents and post--accident modes, with a possibility of its further display and/or recording. Data from an archive are used for assessment of power unit state, detection of short- and long-term changes (trends) of controlled parameters, preparation of reports, further analysis of failure causes, accident progression and mitigation of their effects.

Main *control functions* of I&C systems are the following:

- Protection, limitation, regulation and interlocking performed automatically.
- Discrete control, initiated by other control functions, commands of operating personnel or automatically.
- Remote control, initiated by operating personnel.

Performance of control functions provides in general:

- Assessment of the state of controlled object and environmental conditions.
- Determination of impacts on the controlled object, which are required to achieve control purpose.
- Formation and output of commands for executive elements of technological equipment, which implement control impacts.
- Assessment of achieved control purpose.

Specified actions can be concentrated in one control I&C system or in several interacting I&C systems. For example, obtaining of current data required for performance of control functions can be obtained by other I&C systems, which perform monitoring information functions and generate data for a control system, direct output of commands for executive elements of technological equipment can be performed a by other (executive) I&C systems, providing discrete control functions initiated by commands of the control I&C system.

Protection functions provide timely detection of failures of design specific operating limits and / or conditions of safety operation and output of commands for executive I&C systems and element of technological equipment initiating emergency reactor shutdown, emergency core cooling and residual heat removal, localization of radioactive materials and limitation of accidental release. Protection function has a higher priority compared to other functions of I&C systems.

Limitation functions provide timely detection of failures in design specific operating modes and commands for executive I&C systems or technological equipment elements, on prohibition of modifications (increase or decrease) of specific parameters or initiate their forced return to the limits of the determined range, considered acceptable in current conditions. Limitation functions for example include: generation and output of commands, initiation forced reactor power decrease in the process of planned or unplanned disconnection of technological equipment; opening of pilot safety valve of pressurizer if pressure in the first circuit reached the design limit, etc.

Regulatory functions provide generation and output of commands for executive I&C systems or executive elements of technological equipment to minimize the effect of external disturbances and / or transient processes in the controlled object to controlled parameters of this object. They are required in the process of power unit operating modes, in emergencies, design basis accidents (emergency control) and in the process of post-accident modes. Regulated parameters are, for example, neutron and heat power of the reactor, levels of feed water in steam generators and regenerative heaters, pressure in the main steam header, turbine rotating velocity, etc. The regulation purpose can be maintenance of regulated parameters with a required accuracy on the level of the specified for them set-point or planned change of these parameters with time.

Interlocking functions detect failure of normal operation of technological equipment (overheating, overload, etc.) and / or conditions required for its operation (power supply, cooling, oiling, etc.) and output commands to initiate load decrease or equipment disconnection, preventing its failure. Interlocking functions also include cancellation of fault command execution initiated by other control systems or operating personnel, which could cause damage of technological equipment. Interlocking functions have lower priority comparing to protection functions, except cases, when a lack of interlocking can lead to heavier consequences for safety.

Discrete control functions provide generation and output of commands initiating connection and disconnection of technological equipment or elements of pipe mounting, transfer and shutdown of mechanisms, reactivity control parts and other actions required to change power unit mode (operation in cold and hot standby, startup, power increase, planned shutdown and cooling) or for execution of commands obtained from other control I&C functions. Discrete control commands can be generated upon strict time schedule and/or depending on external events, state of other equipment and results of carrying out previous actions.

Remote control function provides execution of commands and directives of operating personnel by generation and output of control impacts directly to executive elements of technological equipment.

Each I&C usually performs not only main functions, but also auxiliary and service functions.

Auxiliary functions provide continuous automatic check of technical state of systems and their components, related equipment and communication lines; diagnostics, display and archiving of messages on operational events; warnings of attempts of unauthorized access; reconfiguration and restoration of operation after failures, etc.

Service functions support personnel actions in the process of specification and change of set-points, reconfiguration, periodic inspection of system component technical state, etc.

Complexity of I&C systems varies in a wide range – from single-circuit systems of automatic regulation of individual parameters to spatially distributed multiprocessor control computer systems. In addition, possibilities of up-to-date information technologies and available for use element base allow combining many functions, typical for safety systems as well as other (safety related or not important to safety) systems in one system. An example can be a reactor power control, unloading, limitation and accelerated preventive protection system that combines monitoring, regulation of neutron or heat power of the reactor, power limiting, discrete control of unloading reactor, archiving, display, warning and recording and also auxiliary and service functions (failure diagnostics, change of set-points, etc.).

Active in Ukraine regulatory documents NP, 2000 and NP, 2008 divide all NPP I&C systems into two categories: normal operation systems and safety systems.

I&C normal operation systems together with technological systems, equipment and operating personnel control and manage processes in operating mode of the power unit. I&C systems, in particular, perform information and control functions required for automatic control of processes, state of technological systems and equipment, keeping technological parameters in the specified design boundaries, changing power unit operating modes, preventing from violation of operating limits. In the accident and in post-accident period normal operation systems can be used for obtaining information that allows personnel to assess the state of structures, systems and components of the power unit, control the accident and make decisions on mitigation of its effects.

For example, the in-core reactor monitoring system perform direct and / or indirect measurements (calculations) of neutron physical, thermohydraulic and other parameters, defining the state of the core (distribution of neutron flux, energy release field, etc.); checks compliance between the design and current characteristics of the core; alerts personnel about deviation of characteristics from the design values and outputs signals into conjugate normal operation systems that control reactivity; archives and displays the values of core parameters in operating modes, in emergencies, during and after design basis accidents.

The radiation safety monitoring system provides continuous measurement of parameters, defining radiation environment in rooms and on the NPP territory, in sanitary protection zone; archives and displays radiation environment data in each design specific control point; alerts personnel about exceeding of permissible radioactivity discharge into the environment and limits of radiation background.

The reactor power control, unloading, limitation and accelerated preventive protection system, providing automatic reactivity control of nuclear fuel fission processes, safety parameters display system are also related to normal operation systems.

Other examples of functions what I&C normal operation systems perform are:

- Automatic monitoring of constructions and equipment state and control of technological processes (automatic level regulation in the pressurizer; protection against unallowable increase of pressure in the first circuit; monitoring of coolant level in the reactor vessel, coolant leak detection, identification of leak location and assessment of coolant flow due to leak; monitoring of activity and content of isotope-neutron absorbers in primary coolant, etc.)
- Automatic detection and limitation of effects of internal or external hazards considered in the design (fire, earthquake, radioactivity release, violation of terms of safety storage of nuclear fuel and radioactive wastes, etc.)
- Automated control of refueling, displaying data on position, transfer and direction of fuel Assemblies and grabs; monitoring of neutron flux density and concentration of liquid neutron absorber solution; protection against damage, deformation, destruction, or fall of fuel assemblies in the process of their retrieval, relocation, and installation; mechanical interlocking on the margin of permissible relocation or detection of a fuel assembly in non-design position, in case of power loss or occurrence of design specific initiating event.

I&C safety systems together with technological systems and equipment perform safety functions, in accordance with standard IEC, 2011 or Ukrainian regulation NP, 2008, such as emergency reactor shutdown, emergency heat removal, residual heat removal from the core and cooling pool prevention or limitation of discharged radioactive substances over the specified boundaries. Operation of *safety systems* is required in cases, when normal operation systems are not able to keep controlled parameters in design specific operating limits, for example, due to failure, personnel fault or quick and reliable response to deviation of operating limits or safety operation conditions, to prevent development of the emergency into an accident.

Provided there are no violations, the I&C safety systems perform information functions of monitoring, archiving and display of values of controlled parameters, diagnoses its own technical state and alerts personnel about operation failures, which can cause system unavailability to initiate the required safety functions.

The I&C safety systems are involved when specific initiating events, violations of any safety operation conditions occurs, any of the controlled parameters or specified combination of controlled parameters (emergency set-points) exceed design specific limit, and / or on command is obtained from other I&C safety system or from operating personnel.

The I&C safety system that has identified any of the listed causes:

- Alarms operating personnel and displays the cause that initiated the safety function.
- Generates and outputs command or a sequence of commands of design specific protective actions, to executive I&C systems or executive elements (starting devices) of technological safety systems.
- Prohibits executions of commands that could be outputted by other I&C safety systems, I&C normal operation systems and / or operating personnel, provided that they are not compatible with executed protective actions.
- Displays data required for operating personnel for monitoring of safety system

operation, checks accuracy of its operation, and if necessary manually performs permitted safety assurance (duplicate, initiate or interlock commands of protective actions, initiate performance of new safety functions, etc.).

- Archives data of causes that initiated performance of safety functions; commands of protective actions initiated by operating personnel and / or obtained from related systems; of results of automatic diagnostics and detected operation failures.

NPP I&Cs often combine performance of safety and normal operation functions. For example, the neutron flux monitoring system on the basis of results of neutron flux density leak determines relative reactor power, calculates the rate of its change, and when any of these parameters exceed the specified limit, the neutron flux monitoring system generates a signal to initiate performance of preventive protection – normal operation functions, that provides reactor power reduction or prohibits its increase. The value of relative neutron density issued by this system is used in the process of reactor power control function that is also related to normal operation functions. If relative neutron power or rate of its change exceeds the specified emergency set-points, the neutron flux monitoring system generates a signal to initiate performance of safety functions (reactor emergency shutdown).

The combination of safety functions and normal operation functions is also typical for the reactor emergency and preventive protection system and reactor group and individual control rod system. described in further chapters.

COMPONENTS OF I&C SYSTEMS

Individual I&C systems, being relatively isolated parts of the overall I&C system, together perform all I&C functions, interacting with each other, with technological systems and equipment, operating personnel and related NPP I&C systems. Individual I&C system interact with its environment via interfaces separating them. The possibility and efficiency of such an interaction are provided by unification of relevant interfaces, shown in Figure 1, which determine rules of interaction and requirements on devices, providing the required interaction.

Each individual I&C system consists of hardware and software components required for implementation of specified main and auxiliary system functions. Two parts can be emphasized in the structure of modern I&C system:

- *Central Equipment:* Performing, in general, monitoring, archiving, display, recording and output of alarm signals (in control system – also generation and output of protection, limitation, regulation, interlocking, remote control commands). Central equipment of I&C system is a software-hardware complex – complex of independently operated devices, which interact with each other, with peripheral equipment and related I&C systems under control of application programs performing the specified operation algorithms (a device whose features allow its operation in accordance with the specified conditions without placing it inside another device; is traditionally called independently operated.
- *Peripheral Equipment:* Providing conjugation of central equipment with operating personnel, technological systems and

equipment. Peripheral equipment is a complex of devices that are operated independently from each other and can be located at a distance from central equipment.

Moreover, I&C system includes: interface cables; service equipment used in the process of programming, debugging, checking, maintenance on the operating site; internal power supplies; software and operating documentation.

Peripheral Equipment

Peripheral equipment (peripheral or field devices) can be divided on three groups:

- Measurement field devices (sensors), intended for obtaining data on state and / or operation of technological systems and equipment.
- Actuating field devices (actuators), directly influencing starting or regulating elements of technological equipment.
- Elements of manual input, display, alarm (HMI devices), used for visual and audible alarm for operating personnel, input of manual control commands, etc.

Sometimes the impulse lines from the piping or technological equipment to main and blowing valves of pressure sensors, differential pressure and level sensors (together with condensation and leveling vessels and other valves related to these lines) are also related to peripheral devices.

Measurement field devices include temperature, level, flow sensors, pressure and differential pressure measurements, neutron flux measurements, measuring transmitters, etc.

Actuating field devices include motor-, solenoid- and air-operated valves, valve control motors, switchgears, motor control centers, etc.

A peripheral device is usually designed as one independently operated device (rarely – as a group of independently operated parts, structurally and / or electrically interconnected). Operation conditions of the peripheral device (operating and limiting parameters of environment, mechanical effects possible in the process of operation and abnormal natural phenomena, severity grade of the electromagnetic environment in the supposed location, etc.) are design specific which allows defining the safety class, seismic category, group operating conditions and accommodation of each peripheral devices and regulating requirements for it, resulting from this classification.

Peripheral devices of modern individual I&C can be divided into:

- *One-off items*, designed and supplied to NPPs as components of specific I&C systems important to safety.
- *Replicated products*, specially designed as components of not previously determined set of I&C systems important to safety and allowed for use at NPPs.
- *Commercial of the shelf products* of general application, available on the market, the design and manufacturing of which do not intend to use I&C systems important to safety, as components. In English literature, for examples, IAEA, 1999, such items are indicated by abbreviation COTS.

Application of COTS in the structure of I&C systems important to safety is one of the current trends caused by the mass effect of their production and heavy competition of global leaders in information technology field, as a result there is a significant improvement of application properties (accuracy, speed, noise immunity, etc.), relatively low cost, sufficient reliability, approved in different fields of application, independence from one manufacturer, high quality of company maintenance.

At the same time it should be considered that COTS are designed and manufactured without taking into account international and national regulations, rules and standards on nuclear safety and control from state regulatory authorities; information on scope, technique and results of production tests of COTS are nearly inaccessible for users; documents required to assessment of the possibility of safety use of products of general application in the designed I&C system are often absent; relatively small consumption at NPPs comparing to the overall scope of COTS production that does not contribute to establishment of required partnership between their designers and manufacturers, on the one hand, and with an end user – on the other hand. This limits use of commercial of the shelf products in the structure of I&C systems important to safety, in which they are used, as a rule, for performance more complex, but less responsible functions.

Central Equipment (Software-Hardware Complex)

Any I&C system is assembled directly on the operating site of ready-made components, which in the recent past were individual instruments, automation devices and computer devices, communication cables, etc. Integration of hardware and software, debugging and testing of assembled system central part were performed directly on the place of future operation. However, a trend of increasing grade of manufacture components, composing central part of I&C systems, is clearly revealed currently.

Such components are designed, manufactured and supplied to users as plant-manufactured product - software-hardware complexes (SHC), which are more widely used in practice of building I&C systems in different industry branches, including nuclear power engineering. Testing of SHC in the factory environment guarantees that the complex meets all specified requirements, stated in the documents. High grade of manufacture significantly simplifies and speeds up mounting and installation operations and integration of components (hardware and software) of the central part of the I&C system before power unit start-up (Figure 3).

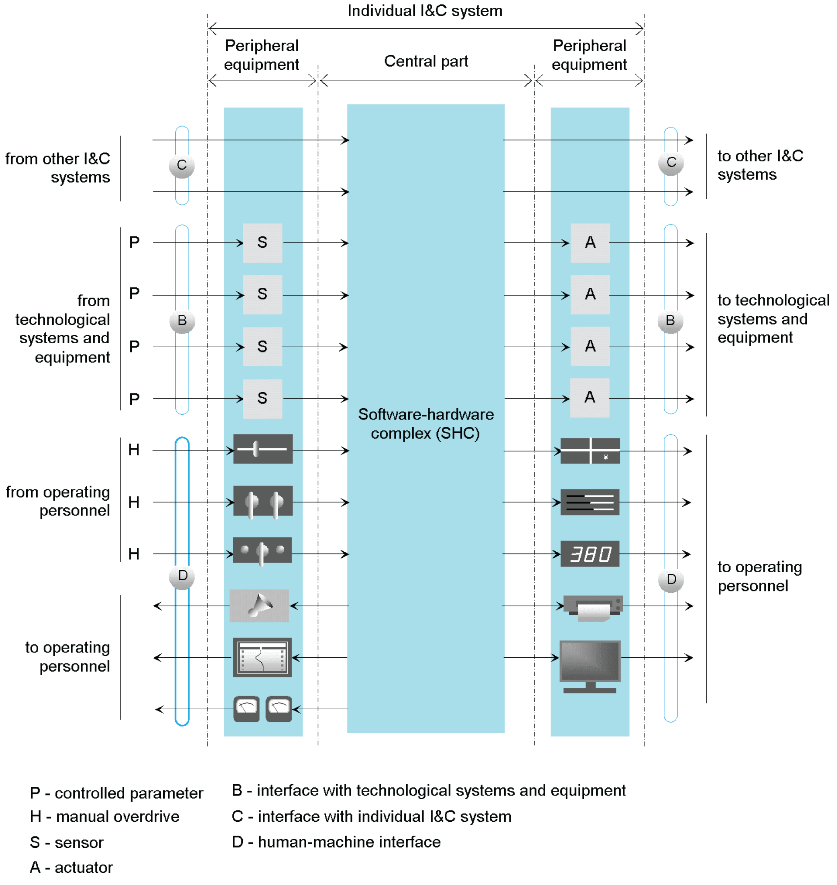
Each SHC is a functionally complete item in the form of one or several independently operated devices with built-in software, which are interconnected through electric and / or optic cables, with peripheral equipment of the same system and with other I&C systems. SHC is usually supplied to the customer as a set with necessary service equipment, repair- and recovery reserve, operating and software documentation. To speed up mounting and decrease the probability of errors, specially manufactured cable items, fully prepared for connecting all entering independently operated devices on the operating place, are often included in SHC structure.

One SHC, being a single component of the system central part that participates in implementation of all its main and auxiliary functions, is often contained in each I&C system. More seldom these functions are distributed among several SHCs, contained in one I&C system, for example, technical diagnostics can be performed by specifically assigned for this software-hardware complexes. To improve reliability several channels are often provided in one SHC and / or several SHCs in one I&C system, which in parallel and independently perform specified functions, providing mutual redundancy.

In general SHC performs:

- Receiving of signals from peripheral equipment (measurement field devices and/or elements of manual input).
- Normalization of discrete signals and transformation of analog signals into digital form.
- Exchange of digital messages with other SHC of the same I&C system and / or with SHC of other I&C systems via communication channels.
- Check of adequacy of obtained information and its processing by the specified algorithms.

Figure 3. Central part and peripheral equipment of I&C system



- Generation and output of control signals to the actuating field devices and signals to the remote HMI-devices, located in the main and emergency control rooms.
- Continuous monitoring (diagnostics) of the technical state of own parts, conjugate peripheral devices, connecting lines and data transmission channels.
- Archiving, display, recording of current and retrospective information and diagnostics result.

Separation of SHC as independent components in composition of I&C systems is due to significant differences between these concepts described further.

SHC is composed of purchased electric and electronic products of general application and devices of own production, as a rule, not independently operated, which are installed in the manufacturing facility in typical supporting structures (shells) in accordance with engineering documentation of SHC. Before delivering to the customer, the manufacturer performs a full inspection of SHC operation with emulators of peripheral equipment and on the basis of results confirms compliance of supplied SHC with requirements of current regulations, rules, standards and the specification, agreed with the customer. Additional inspection (preoperational tests) of SHC is performed on the operating place before integration with peripheral equipment of I&C

system. The manufacturer's warranties cover SHC as a whole, including purchased component parts applied in it. In the process of modernization of the I&C system the entire SHC is usually replaced.

In contrast, I&C system is composed of independently operated devices (products), obtained in accordance with customized specification; their mounting, connection and installation are performed in accordance with project documents of I&C system on operating place. Joint operation of devices, forming a central part of I&C system, can be inspected only on operating place, after mounting and integration of all its components (hardware and software). The supplier guarantees apply to each product individually, but not to all I&C system. In the process of I&C system modernization only a part of equipment is usually replaced (for example, many peripheral devices, connecting cables, etc. are left).

There are significant differences in both software SHC and I&C system. Software SHC is its integral part and designed by the same organization as for SHC. In the process of design of software its verification, including checking after integration with hardware SHC, is provided. Saving of program in read-only memory and further checking of SHC operation are performed on the manufacturing facility before delivery to the customer. Downloading or modifying of programs in the process of integration of SHC with the peripheral equipment and installation of I&C system is often not required.

And conversely, software of I&C systems is interpreted as a set of programs, saved in read-only memory of SHC and all software-hardware peripheral devices (if applicable), and also service programs in machine-readable mediums, intended for checking of operation of I&C system and contained in it individual devices. These software components are designed by different organizations at different times and independently, component integration and further software checking can be performed only on the operating place of the I&C system.

Independently operated devices, being component parts of SHC, can play different roles for safety and can be operated in different conditions, so the safety class, seismic category, group operating conditions and accommodation and resulting classification requirements for resistance to external influences, noise immunity, quality of electric isolation, etc. can be defined for each component parts individually, but not for SHC as a whole.

Software-hardware complexes of modern individual I&C systems can be divided into:

- One-off items, each is designed, manufactured and supplied to NPPs by individual order as a component of individual I&C and cannot be directly (without any modifications) used in other systems.
- Replicated products, designed as components of I&C systems important to safety that were not of not preliminary defined, .allowed for use at NPPs and do not require any significant modifications of hardware and/or software in the process of manufacturing and supply for use in different industry branches.

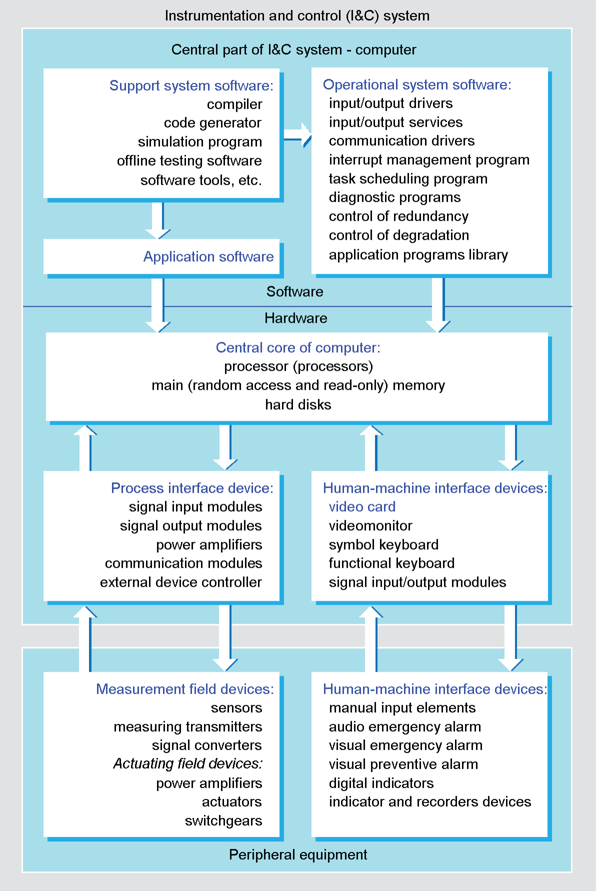
Software of I&C Systems

Software is considered as one of the components in I&C systems, starting from the time, when all-purpose control computers were used for performance of the main system functions. At Ukrainian NPPs such an approach was first implemented in information systems, developed on the basis of serial produced computer CM-2M, which was intended for application in automated systems, manufactured in different industry branches. System software, providing operation and maintenance, was supplied in composition of CM-2M. Application software, directly connected with the tasks of process control and monitoring, was usually developed independently from the supplier of CM-2M.

System software is usually divided into two parts: operational software (programs directly executed in the process of operation) and support software (programs used during design, testing and maintenance of operational software and computer hardware). Examples of operational software: input/output and communication drivers; interruptions management programs; job scheduling software; programs for the diagnosis and management of redundancy in case of failures; library applications programs. Examples of support software: compilers, code generators, software offline testing, software utilities, etc. The developed application programs were usually integrated with operational software and hardware directly on the operating place. Integration and further checking (verification) took place in critical shortage of time which complicated detection of faults that could be made during applications software design. Defects made during software design and not detected during verification, could reveal themselves under specific conditions during operation and cause failure of functions performed by the I&C system.

Typical features of the described approach to the design of software for I&C systems (Figure 4): orientation at a single computer in the system ; storage of all executable programs in the memory of this computer; clear separation between the system and application software; design of system and application software by different organizations. Insufficient reliability of the first

Figure 4. Hardware and software of I&C system with centralized structure



universal computers, low operating speed, significant labor expenditures in design and debugging of application software, high probability of "hidden" defects, programming errors and impossibility of comprehensive testing of application software by the developer did not allow using such computers in NPP safety systems.

Significant extension of a set of software performed functions for NPP units was provided, first, by element base development—appearance of available for use microprocessors, single-chip microcomputer and microprocessor controllers, including one or several microprocessors together with the relevant memory, for which IEC, 2008 suggested a more general title programmable electronic. (In this standard control, protection and monitoring system, based on one or several programmable electronic devices, is called a programmable electronic system).

It became possible to perform functional decomposition- division of complex function into a set of significantly simpler ones: the calculating possibilities and storage capacity of appeared at that time programmable electronic devices. For examples, functions of input and input signals transformation; comparison with set-points; functions of logic processing and generation of control commands; functions of continuous monitoring of technical state, etc. could be assigned. Along with functional decomposition, structural decomposition, providing participation in performance of one function of several sequentially or parallel connected programmable electronic devices, was used. For example, input and transformation functions in case of large number of input signals can be performed not by one, but by several simultaneously operating devices, among which all input signals are distributed; diagnostics function of technical state of system parts can be performed under control of software, directly containing in each of these parts; results of check can be transferred for further processing, display and archiving by specifically assigned programmable electronic devices, etc.

Such an approach for building programmable electronic system, called "distributed" or "decentralized" control, allowed refusing from central computes and replacing them with a set of programmable electronic devices, distributed throughout the system. It is considered that such a device individually has low complexity in the sense of that all types of failures of each of its components are clearly determined, and the device's behavior, in case of defects, is fully determined. The simplicity and relative independence of performed functions cardinally simplified the design of software for programmable electronic devices of low complexity and allowed to refusing from use of operation system, software interrupts, drivers, etc. Important factors are lower probability of errors during design and relatively simple determination of defects in the process of software testing (before supplying to the customer). So, typical software features of modern I&C systems are: orientation at many programmable electronic devices, included in a system; storage of executable programs directly in the memory of these devices; elimination of the differences between a system (operating) and application software; combination of hardware and software design for these devices, simultaneously performed by one and the same organization; integration of hardware and software directly on manufacturing place and supply of programmable electronic devices with "built-in" software. Distribution of functions between hardware and software made by developers is often not reflected in operating documentation, i.e. is left unknown to the user. This software can be changed only by replacing the device, containing previous software, with a new one with modified software (IEC, 2007,b).

As a result of the specified peculiarities, it became possible to implement software for implementation of main functions of I&C systems important to NPP safety. In the second half of the eighties programmable electronic systems, developed by Electricite de France, performed not only information and support functions, automated regulation, logic control, but also reactor protection functions. Similar tasks were solved by Westinghouse Electric Company at NPP Sizewell B in England and also by Canadian corporation Atomic Energy of Canada Ltd. at NPP Darlington-A. In 2002-2003 Westinghouse Electric Company imbedded overall I&C systems in two power units of Czech NPP Temelín, in which software methods for reactor protection, power regulation, reactor power limitation, in-core reactor monitoring, control of technological equipment, information display in main and emergency control rooms and radiation safety monitoring were used. Also programmable electronic devices were widely used in systems implemented by Siemens Power Corporation within the last 12 years at a number of European NPPs and at power units in China.

Programmable electronic devices at USSR NPPs were first used in automatic turbine control systems, developed in the early 1980-s. Nowadays, at most Ukrainian power units all main functions of reactor control and protection are performed by software-hardware complexes based on programmable electronic devices.

SHC software is a set of programs, which:

- Control operation of all components of SHC, provide their interaction with each other, with conjugate peripheral devices and other SHCs.
- Provide performance of human-machine interface functions.
- Diagnose components of SHC, conjugate peripheral devices and connecting lines during power-up and operation.
- Automate checking of proper operation of components of SHC and calibration of measuring channels in the process of maintenance and after recovery.
- Support personnel actions during reconfiguration of SHC (change of set-points, blocking of command generation, etc.).
- Prevent personnel errors during reconfiguration, maintenance and recovery of SHC.

Application and system software is located in SHC components – on hard discs in read-only and random-access memory and / or in logic structures of complex programmable electronic components, supports software – on external carriers and/or in memory of service components. SHC software also includes copies of current program versions on external carriers and software documentation. Development of electronic projects of complex programmable electronic components is usually considered as one of programming types, though it is slightly different from point of view of requirements to design and verification – see Kharchenko & Sklyar, 2008.

Figure 5 shows an example of interaction of hardware and software SHC.

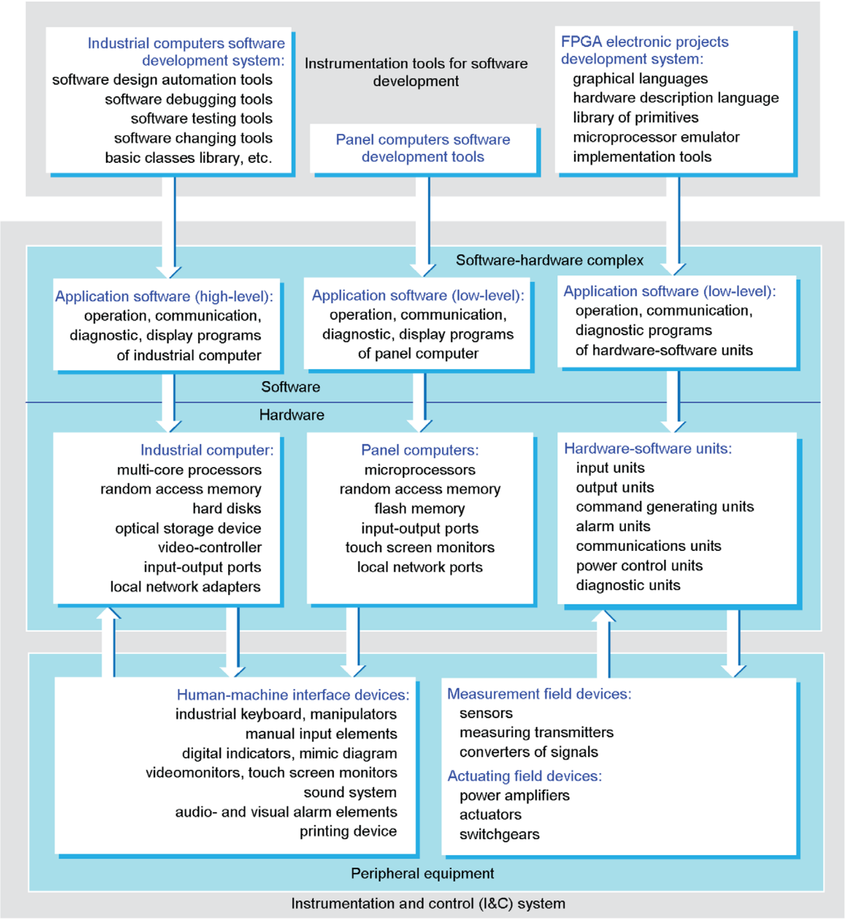
EQUIPMENT FAMILIES

Equipment family (equipment platform) is set of hardware and software components that may work co-operatively in one or more defined architectures (configurations).

The purpose of equipment family creation – provide a possibility to use uniform hardware containing into equipment family during design and packaging of SHC or I&C systems instead from of separate items of different suppliers (often not compatible with each other and not always conformed to system requirements). The equipment family is characterized by:

- Functional, structural and constructive completeness for the main field of application of this equipment family.
- Informational, power, constructive, operational and other types of compatibility.
- Advanced software, metrological, standard-methodological, informational and other types of support.

Figure 5. Hardware and software of I&C system with distributed structure


Industrial computers software development system:
software design automation tools
software debugging tools
software testing tools
software changing tools
basic classes library, etc.
Instrumentation tools for software development
Panel computers software development tools
FPGA electronic projects development system:
graphical languages
hardware description language
library of primitives
microprocessor emulator
implementation tools
Software-hardware complex
Application software (high-level):
operation, communication, diagnostic, display programs of industrial computer
Application software (low-level):
operation, communication, diagnostic, display programs of panel computer
Application software (low-level):
operation, communication, diagnostic programs of hardware-software units
Software
Hardware
Industrial computer:
multi-core processors
random access memory
hard disks
optical storage device
video-controller
input-output ports
local network adapters
Panel computers:
microprocessors
random access memory
flash memory
input-output ports
touch screen monitors
local network ports
Hardware-software units:
input units
output units
command generating units
alarm units
communications units
power control units
diagnostic units
Human-machine interface devices:
industrial keyboard, manipulators
manual input elements
digital indicators, mimic diagram
videomonitors, touch screen monitors
sound system
audio- and visual alarm elements
printing device
Measurement field devices:
sensors
measuring transmitters
converters of signals
Actuating field devices:
power amplifiers
actuators
switchgears
Peripheral equipment
Instrumentation and control (I&C) system

The specified peculiarities allowed building various software-hardware complexes on the basis of one and the same equipment family for overall or individual I&C systems, different by a composition, structure, technical characteristics, meeting requirements of individual customers, and at the same time provide rational use of means and work efficiency during design, programming, manufacturing and operation of these SHCs. (This does not exclude a possibility of technically and economically grounded cases of adopting individual; purchased items, not included in the composition of equipment family).

It is appropriate to mention fundamental differences between the equipment family and SHC. The equipment family is a conceptual object and exists only as an engineering, software or technological documentation, methods, instructions, standards, etc. The same equipment family generates a set of various SHCs, where each is a real object (product of industrial manufacturer). The equipment family is not bound to any specific system: it is intended for typical functions, structures, environment, ways of use and operating conditions, common for a sufficiently wide, though restricted range of different systems. Each SHC that can be implemented on the basis of equipment family is usually devoted to one specific system. Separately taken SHC uses only a part of possibilities of a relevant equipment family (restricted nomenclature of hardware and software, supporting constructions, signals, interfaces, etc., required and sufficient for a specific application).

The equipment family is usually oriented for performance of a set of typical functions, which can be selected, gathered in various combinations, and customized according to tasks of the specific I&C system. The design of hardware and application software of SHC is supported by relevant tools and supports software, recommended or supplied by the equipment family designer.

The equipment family can be a product of a certain manufacturer or a set of items, gathered and adapted by supplier. Marketing policy of equipment family designers can provide one or several options of use for building SHC:

- Delivery of separate items from the equipment family; in this case integration of equipment family components and adaptation of SHC for performance of specified functions (including, when required, completing a set with items of another manufacturer) are performed by the customer (end user or organization that assembles and supplies of SHC to the end user).
- Supply as a basic part of SHC; in this case the supplier (and also the designer of equipment family) integrate of those components of hardware and software, that are directly specified in contract; adaptation for performance of specified functions (design of application software and its integration with a basic part of SHC) is performed by the customer.
- Supply as a complete SHC; in this case the supplier (equipment family designer) himself determines components of hardware and software required for performance of functions specified by the end user, develops application software and performs integration of all component parts and testing of SHC. The end user obtains a fully debugged and tested “turnkey” SHC.

Some organizations prefer not provide free access to developed documentation and hardware. Having a set of aggregate modules, supporting structures, basic programs, instrumentation tools and typical methods, and using them during assembling of SHC for various I&C systems, they do not register and advertise this set (having all features of equipment family) as a public platform, using it only for development of their own SHCs .

Many companies actively use such an approach for meeting individual users’ needs, building relevant equipment families. Development was preceded by researches, which detect real problems and needs of a certain group of users, then on their basis technical requirements able to efficiently meet these needs, are developed. Due to the considered ideology, optimal set of equipment and availability of all required types of provisions, this platform is more valuable for the end user, than a simple set of its components. In the composition of equipment family more or less external components are also used: standards, technologies, design automation facilities, marketing initiatives, infrastructure of tracking and maintenance, etc. For platform will to gain a real value, all its components should be compatible and well combined with each other.

WDPF-II - equipment families of Westinghouse Electric Company intended for building distributed I&C systems with a wide choice of applied use. In WDPF-II a long experience of development and operation of earlier generation equipment in power units with Pressurized Water Reactors (PWR), manufactured by the same company, is accumulated.

Lower level is based on several operating stand-alone devices- Distributed Processing Units (DPU). Each DPU contains two redundant microprocessor controllers and a set of input-output modules of analog and discrete signals. Controller is implemented on the basis of processor architecture IA-32 (Intel Corporation) and contains microprocessor, flash-memory, random access memory, watch dog. Input-output modules are connected to both controllers. DPU captures information about parameters of technological processes from sensors and transmitters; performs linearization, scaling and transformation of analog signals into digital form; storage and processing of digital data; generation of control, protection and interlocking signals; transfer of information to an upper hierarchical level. Diagnostics, automatic restart, configuration possibility, off- and on-line control and readjustment are also provided.

Devices (sub-complexes) of upper level are implemented on the platform of workstations manufactured by Sun Microsystems, Inc. with a real time operation system Solaris. Workstation contains processor, random access memory, disc memory, controllers of Ethernet dataway, sequential and parallel ports. Depending on subcomplex purpose, it can contain one or two video monitors with relevant graphics controllers (video cards), alphanumeric and / or function keyboard, manipulator, ink and laser printers, acoustic system. Subcomplexes of upper level archive, display, record data, prepare and output messages for NPP computer information system. For complex computations, which require high operating speed, a significant capacity of random access memory and on-line database access, industrial personnel computer is included into the proper subcomplex.

All operating stand-alone devices of lower and upper level are connected by a common redundant 32-bit digital network Westnet-II Plus Data Highway with trunk line topology, deterministic access to communication environment and communications protocols. Such a solution provides simple implementation of distributed database, but requires expensive hardware and imposes limitation on a total number of controlled parameters. Both trunks of Westnet-II Plus network operates simultaneously; when one of them fails, the system keeps operability without degradation of characteristics. Via local Ethernet network servers of upper level can transfer and obtain such information, for which possible communication delay (program load, transfer of archival data, printout) is not critical.

In Ukraine on the basis of WDPF-II modernization of information systems of units 1 and 2 South-Ukrainian NPP, upper level of in-core reactor monitoring system of unit 2 Zaporozhe NPP, regulators of feed water level in steam generators of units 1 and 3 South-Ukrainian NPP was performed. Systems, providing parameters of vibration monitoring of main circulating pumps in unit 3 Rovno NPP and safety parameters display systems at all Ukrainian units were designed and introduce into operation.

OVATION — platform of Westinghouse Electric Company, that replaced WDPF-II. Instead of original network Westnet-II Plus it uses token-ring network with a standard interface FDDI (Fiber Distributed Data Interface). Fiber-optic cable with two optical fibers is recommended as a physical communication environment. One of it forms a main ring, and it is used for circulation of marker and data. The second fiber forms a standby ring, and in normal mode it is used for control of communication via the main ring. In case of failure (break) of any segment of the main ring, stations, being on both sides of break, will automatically reconfigure path of marker and data circulation, connecting standby ring. Also FDDI standard regulates other features, providing network fault tolerance. Protocol's determinacy (possibility to predetermine maximum delay of package transmission via network) is especially important for control systems critical to information transfer period.

In stations of lower level controller is implemented on the basis of processor architecture IA-32, dominating on personnel commuter market in the period of OVATION development. Real time operation system supports multitask mode and operation with task priorities. For reliability improvement controllers can be duplicated, where the main controller operates in control mode and, moreover, checks operability of the duplicating controller and network; at the same time the duplicating controller checks operability of main one and monitors current database, which allows bumpless switching to duplicating controller, when the main fails. For connecting controllers to network of FDDI, special-purpose network adapters are used. Input-output modules of analog and discrete signals have built-in microcomputers and can be duplicated or reserved on logic condition "two-out-of-three." During the use of fiber-optic communication lines, it is possible to move input-output modules on 2 km from a controller. Instead of any input-output modules, single-loop regulatory module, communication module, rotation velocity detector, controller valve positioner can be connected to a controller.

Upper level is formed by workstations, implemented on the basis of personnel computer with a processor Pentium IV or Sun Blade 150, operation system Windows NT or Sun Solaris (correspondingly), random-access memory, disc storage, special operator's keyboard. In work stations interfaces for direct connection to FDDI network are provided.

Engineering workstation performs configuration and software maintenance functions, stores system programs and source codes of application programs. Workstation of archiving and recording is implemented on platform Ultra Sparc Station under operation system UNIX. It stores data about measured values, events, operator's actions, etc.

In the whole world hundreds of information and control systems, based on platform OVATION, are developed and implemented in power engineering and other branches. In Ukraine OVATION is used in safety parameters display systems at Zaporozhe NPP.

As far as equipment families OVATION are not certified for use in safety systems, Emerson Process Management implements such systems on AC 160 platform (earlier Westinghouse Electric Company used platform Eagle for safety system). In particular, on the basis of AC 160 reactor protection system in Ringhals NPP unit 2 (Sweden) and safety systems in Ulchin NPP units 5 and 6 (South Korea) were implemented.

TELEPERM XP and *TELEPERM XS* - equipment families, developed by Siemens Power Corporation as a technical base for central part of information and control systems, including systems important to safety. Platform TELEPERM XP is oriented at application in normal operation systems, TELEPERM XS – in NPP safety systems.

Among other foreign platforms Common Qualified Platform (Common-Q), developed by ABB Nuclear Automation (Westinghouse Electric Company uses modified version of this platform - Westinghouse Advant), and Tricon programmable logic controller system (Tricon PLC) of Triconex Corporation are also should be mentioned.

In Ukraine during assembling of new software-hardware complexes to be supplied on NPP, platforms of foreign companies are nearly not used currently.

First *Ukrainian equipment families* were developed more than 30 years ago. In 1983, at International exhibition "Automation-83," placed in Moscow, an aggregate complex of technical means (platform) MikroDAT, widely used in various industry branches and in nonindustrial field (Didenko & Rozen, 1985), was presented. Typical characteristics of this platform, further developed in modern Equipment family, should be mentioned:

- Implementation of concept of distributed control, based on use of large integrated circuits, microprocessors.
- Optimization of nomenclature of aggregate modules (functionally complete, structurally standalone items with unified external communications).
- Standardization of the main and joint size of aggregate modules and switching elements for external connections.
- Specific assembly items for placing, mechanical protection, electric integration and connection of aggregate modules to external chains.

- Constructional aggregation on several assembly levels (module units, assembles of modules, devices, software-hardware complexes).
- Standardization of input / output signals, communication interfaces and protocols between aggregate modules.
- Consistency of requirements to items by resistance to external factors typical for industrial operation conditions.
- Software, standard-methodological provision, information provisions, service and instrumentation tools.
- Development of concepts of design of object- and problem oriented assembles of modules, devices, software-hardware complexes.

At present, during design and packaging of I&C systems at Ukrainian NPPs several equipment families are used.

RADIY PLATFORM (Bachmatch, 2008) – equipment family of Research and Production Corporation Radiy. Its main peculiarities are: use of Field Programmable Gate Arrays (FPGA) in function blocks of lower level to perform main functions; use of programmable electronic devices built-in in the same blocks for independent performance of auxiliary functions (control, diagnostics, etc.); primary use of fiber-optic lines for data exchange between component parts of SHC; use of industrial servers, panel computers, uninterruptable power supply for exchange of message, archiving, display, recording, database maintenance, etc. in workstations,

RADIY PLATFORM has two-level structure. Lower level is formed by typical cabinets:

- Normalizing (obtain and normalize discrete signals, continuous standard DC signals and signals of thermoelectric converters, and also provide galvanic separation of chains and power supply for sensors).
- Signal generation (transform input signals into digital form, process data and generate output signals according to specified algorithms).
- Cross output (generate and output commands by results of logical processing of signals, obtained from three signal generation cabinet according to logical condition “two-out-of-three”).
- Remote control (actuators control by commands of automatic regulators, technological protection and interlocking, obtained from signal generation or cross output cabinets and by commands of operating personnel).
- Alarm (commands, which control process signaling board in the main- and emergency control rooms).
- Position monitoring (determine control rod positions and output proper signals to remote control cabinets and indication elements, located in the main and emergency control rooms).
- Power supply (provide primary power supply to software-hardware complexes and force power supply by alternating and direct current for control rod drives; terminate force power supply by command of reactor protection or accelerated preventive protection, obtained from cross output cabinet).

Cabinets include modular units to input standardized analog signals, signals of thermoelectric transmitters and digital signals, of generation control commands, diagnostics, alarm, optical communication and transmission of optical signals, selection of interlocking, actuators control, etc.

Upper level of RADIY PLATFORM is formed by workstations, which:

- Receive technological information and diagnostic messages from cabinets of lower level.

- Generate alarming messages in cabinet of normal operation failures and detection of defects and failures of lower level cabinets.
- Archive, display and recording or technological information, input and output signals, commands and diagnostic messages.
- Maintain human-machine interface.

RADIY PLATFORM-based SHC and I&C systems are described in the next chapters.

WULKAN - equipment family, intended for use in I&C systems, is a Ukrainian version of Westinghouse Distributed Process Family (WDPF-II) of Westinghouse Electric Company.

Manufacturing and supply are performed in the form of complete SHCs (with integrated system and application software) or as a base part of SHC (with system software, which composition is determined by contract). In the second case application software is developed by third-party organization and integrated with a base part SHC.

Under control of system software, in real time SHC performs the following main functions (including the possibility of redundancy):

- Reception and output of electric analog and discrete signals.
- Reception and execution of commands of operating personnel.
- Exchange of messages with other SHCs and / or I&C systems via digital communication channels.
- Processing, archiving, display and recording of current and archived data.

Auxiliary functions provide continuous monitoring of technical state of SHC, output of diagnostic messages, hardware access monitoring, reception and output of standard time signals (if necessary).

The main elements of aggregation during assembling of WULKAN-based SHC are sub-complexes, designed as independently operated devices in on-floor or wall hanging cabinets, tables, and crates:

- Sub-complexes of data acquisition and processing on DPU platform, contained in equipment family WDPF-II.
- Sub-complexes of workstations on the base of industrial computers of Sun Microsystems, Inc. (USA).
- Sub-complexes of hubs.

Sub-complexes have variable composition and are assembled from a set of technical means, included in equipment family WULKAN: modules for transformation of continuous and discrete signals; galvanic separation devices; controllers of local networks Ethernet, RS-485, Westnet-II Plus Data Highway; magnetic and optical disc storages; monitors, keyboards, printers, etc. During supply of complete SHC, composition of each sub-complex is determined by performed functions, number and type of input and output signals, necessity of redundancy and other requirements. During supply of base part of SHC, composition of each sub-complex is specified by the customer directly in a contract. Combination both electric and fiber-optic cables can be used.

On the platform WDPF-II software-hardware complex for computer information system in South-Ukrainian NPP unit 1(Afanasiev, 2002) was designed and manufactured, which then was integrated with safety parameters display system (Anikanov, 2003). Similar by purpose and performed functions SHCs were designed on the platform WULKAN and implemented by Ukrainian corporation “Westron” (Belohin, 2007) in other Ukrainian units. Software-hardware complexes designed on the same platform are operated in radiation monitoring systems of Zaporozhe NPP.

WULKAN-M – a new equipment family, manufactured by corporation "Westron" for subcomplexes of data acquisition and processing. In contrast to the analogue (DPU), equipment family WULKAN-M allows assembling software-hardware complexes not only for normal operation systems, but also for safety systems. WULKAN-M-based SHCs can receive process and output analog and discrete signals and / or digital messages. Redundancy of the main functions, including the use of hardware and/or software diversity in redundant channels, is possible. During assembling of WULKAN-M-based SHC, built-in electronic modules, industrial computers, power sources, fan units, designed and manufactured by SHC supplier, and purchased component parts (processor circuit board and peripheral equipment of industrial computers, communication adapters, controllers of peripheral devices, local network equipment, etc.) are used. For placing, electrical interconnection and connection to external circuits of built-in component parts, typical supporting structures - crates and on-floor cabinets are used. Each SHC is assembled and produced in accordance with customized technical requirements, which determine safety class, performed functions, number and type of input / output signals, necessity of redundancy, etc.

On the basis of equipment family WULKAN-M, SHCs for I&C systems of feed water level regulation in steam generators, which were put into operation in South-Ukrainian NPP units 1, 2 and 3, setting in operation emergency diesel generators, etc. are were developed. Development of equipment family WULKAN-M allowed using it as a platform for lower level hierarchical I&C systems, in which upper level can be implemented on the basis of other equipment families. Such an approach was accepted, for example, during modernization of computer information system of South-Ukrainian NPP unit 3, in which subcomplexes of data acquisition and processing were assembled on the platform WULKAN-M, and an upper level was implemented by Westinghouse Electric Company on the basis of equipment family OVATION.

Among other equipment families, developed and applied in Ukraine and include in systems important to safety, control computer complexes MSKU (final versions allow assembling, including fault tolerant of safety class 2) and complex of workstations PS 51XX, on the basis of which an upper level of hierarchical systems, including automated workplaces of operating personnel, are implemented, can be also named.

Solutions and Recommendations

There are common tendencies in development of I&C systems in all countries - NPP's operators. But a lot of these countries have own technical decisions in NPP I&C creation. Ukraine belongs to these countries: Ukraine imported I&C systems as far back as 10-15 years ago. After that full modernization of Ukrainian NPP I&C took place and Ukraine became to export NPP I&C systems and appropriated equipment to NPP in different parts of the world: not only to Europe, but to America and Africa.

Therefore authors can recommend this book to readers for acquaintance with Ukrainian experience in NPP I&C elaboration: this experience will be described in chapters 2-13.

FUTURE RESEARCH DIRECTIONS

Let us mention some areas of activities from their range required for further development of NPP I&C systems.

1. Application of complex electronic components, using Hardware Description Language (HDL). They include Application Specific Integrated Circuits (ASIC), Complex Programmable Logic Devices (CPLD) and

Field Programmable Gate Array (FPGA). Several FPGA-based systems, considered in further chapters, were developed.

2. Because of the wide use of digital I&C systems at NPPs the issues of cyber security should be taken into account in the process of development, implementation, operation and safety assessment of these systems. Thus, the important directions for future research are:
    a. Analysis of international experience in the field of cyber security.
    b. Development of requirements on cyber security and including them into international and national standards and regulations.
    c. Implementation of cyber security measures in NPP I&C systems for prevention of malicious unauthorized access, modification or damage of data and software, which could lead to accident, incorrect operation or loss of important information.
    d. Development of methods for assessment of safety, completeness and correctness of cyber security measures in the process of the licensing process.

Some issues of cyber security are considered below.

3. Aging of specialist and loss of knowledge are the actual problems in the field of NPP I&C. It is important to implement the knowledge management into activity of organizations that design, manufacture, operate or make safety assessment of NPP I&C systems. It should include the following:

    a. Development and implementation of the knowledge management program in each organization which involved into activity in the field of NPP I&C.
    b. Development of methods for capturing, documenting and saving the tacit knowledge of experts in field of I&C.
    c. Permanent training and tutoring for transfer of knowledge from experienced experts to young specialists.
    d. Development of national and international knowledge portals at NPP I&C for improving the cooperation between the different organization.

Some issues of knowledge management are considered below.

4. One of the research trends, dictated by effects of accident at NPP Fukushima, is the development of sensors able to sustain extreme environmental impacts, in case of accidents inside the reactor containment. These sensors are required to be qualified under conditions of high temperature, high radiation, and aggressive environment.
5. Application of wireless sensors, decreasing costs for routing and maintenance of cables. There are the following problems:
    a. Resistance of wireless devices to electromagnetic and radio frequency noise.
    b. Cyber security in case of unauthorized access to wireless channels, transmitting information from the outside, for interception, blocking, intentional distortion of signals or output of spurious signals to receivers.
    c. Integration of wireless equipment with current instrumentation and control systems and communication networks, etc.

CONCLUSION

Chapter 1 contains common information about I&C systems and their functions, safety and safety related (normal operation) systems, components of I&C systems (central part, peripheral equipment, software), equipment families, etc). However even from this chapter can be included that problems of NPP I&C safety were, are and will be actual. The confirmation of that is the experience of big accidents in NPPs: Three Miles Islands, Chernobyl and Fukushima, which changed requirements to NPP as whole and to NPP I&C particularly.

Chapter 1 with common information contained the main future directions. Note only three from them.

Problem of NPP life extension are belonging more and more actual for the most countries- NPP-operators (USA, Canada, Russia, Ukraine, etc). Decision of this problem is impossible without wide I&C modernization.

Fukushima lessons have to be learned (development of sensors able to sustain extreme environmental impacts inside containment in case of accidents, the application of the wireless sensors; improvement of seismic resistance, etc).

Computer technology is susceptible to a number of cyber threats, (what are changed quickly-remember STUXNET worm) and the issues of cyber security should be taken into account in the process of NPP I&C development, implementation, operation and safety.

REFERENCES

Afanasyev, N., Belohin, O., Brenman, O., et al. (2002). Maintenance and safety assessment of computer information system of NPP unit with WWER-1000 reactor. *Nuclear and Radiation Safety, 4*.

Anikanov, S., Bezsalyj, V., Belohin, O., et al. (2003). Maintenance and safety assessment of nuclear power plant safety parameters display systems of WWER-1000 reactor. *Nuclear and Radiation Safety, 1*.

Bakhmach, E., Siora, A., Bezsalyi, V., & Yastrebenetsky, M. (2008). Digital systems for reactor control: design, experience of operation. In *Proceedings of the 16th International Conference on Nuclear Engineering*. Orlando, FL: ICONE16.

Belohin, O., Brenman, O., Kudinov, Yu, et al. (2007). Reconstruction of computer information system of South-Ukrainian NPP. unit 2. *Nuclear and Radiation Safety, 1*.

Cluley, J. C. (1994). *Reliability in instrumentation and control*. London: Butterworth Heinemann.

Didenko, K., & Rozen, Y. (1985). MikroDAT: Principles of construction, the main parameters and characteristics. *Instrumentation and Control Systems, 11*.

IAEA. (1999). *Modern instrumentation and control for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (2007). *Terminology used in nuclear safety and radiation protection: IAEA safety glossary*. Vienna, Austria: IAEA.

IAEA. (2011). NP-T-3.12. *Core knowledge on instrumentation and control systems in nuclear power plants*. Vienna, Austria: IAEA.

IEC. (2007a). IEC 60050-394. *International electrotechnical vocabulary - Part 394: Nuclear instrumentation – Instruments, systems, equipment and detectors*.

IEC. (2007b). IEC 60987. *Nuclear power plants – Instrumentation and control important to safety –Hardware design requirements for computer-based systems.*

IEC. (2008). IEC 61508. *Functional safety of electrical/electronic/programmable electronic safety related systems: Part 4: Definitions and abbreviations.*

IEC. (2011). IEC 61513. *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*.

Kharchenko, V., & Sklyar, V. (Eds.). (2008). *FPGA-based NPP: Instrumentation and control systems: Development and safety assessment. National Aerospace University KhAI*. State Scientific and Technical Centre for Nuclear and Radiation Safety.

NP. (2000). NP 306.5.02/3.035. *Nuclear and radiation safety requirements to instrumentation and control systems important to nuclear power plants safety*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2008). NP 306.2.141. *General provisions on the safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Committee.

Rosenberg, M., & Bobryakov, S. (2003). *Elsevier's dictionary on nuclear engineering*. London: Elsevier Science.

Smith, J., & Simpson, K. (2001). *Functional safety: A straightforward guide to IEC 61508 and related standards*. Oxford, UK: Butterworth Heinemann.

Storey, N. (1996). *Safety-critical computer systems*. Reading, MA: Addison Wesley Longman.

Yastrebenetsky, M., Vasilchenko, V., & Vinogradska, S. et al. (2004). *Nuclear power plants safety: Instrumentation and control systems*. Kiev: Technika.

ADDITIONAL READING

Booher, H. R. (2003). *Handbook of Human Systems Integration*. Wiley. doi:10.1002/0471721174

Courtois, P.-J. (2008). *Justifying the Dependability of Computer-based Systems*. (With Application to Nuclear Engineering). Springer.

DI&C-ISG-01. (2007). *Cyber Security. Interim Staff Guidance on Digital Instrumentation and Control*, Cyber Security, US NRC.

DI&C-ISG-02. (2009). *Diversity and Defense-in-Depth (D3). Revision 2, Interim Staff Guidance on Diversity and Defense-in-Depth Issues. Interim Staff Guidance on Diversity and Defense-in-Depth Issues*, USNRC.

DI&C-ISG-03. (2008). *Risk-Informed Digital Instrumentation and Controls*. Interim Staff Guidance on Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments, USNRC.

DI&C-ISG-04. (2009) *Highly Integrated Control Rooms & Digital Communication Systems.* Revision 1, Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc), USNRC.

DI&C-ISG-05. (2009). *Highly Integrated Control Rooms & Digital Communication Systems.* Revision 1, Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc), USNRC.

DI&C-ISG-06. (2009). *Licensing Process* Licensing Process Interim Staff Guidance, USNRC.

Dunn, W. R. (2002). Practical Design of Safety-Critical Computer Systems, Reliability Press, Solvang. USA.

EPRI. 1008124. (2004). *Practical Maintenance of Digital Systems*, Electric Power Research Institute, Palo Alto, CA, USA.

EPRI. 1011851. (2005). *Guidance for the Design and Use of Automation in Nuclear Power Plants, Electric* Power Research Institute, Palo Alto, CA, USA.

EPRI. 1015313. (2010). *Computerized Procedure Systems: Guidance on the Design, Implementation, and Use of Computerized Procedure Systems, Associated Automation, and Soft Controls*, Electric Power Research Institute, Palo Alto, CA, USA.

Gertman, D. I., & Blackman, H. S. (1994). *Human Reliability and Safety Analysis Data Handbook*. New York, USA: John Wiley and Sons.

Hashemian, H. M. (2005). Sensor Performance and Reliability, ISA—The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

Hashemian, H. M. (2006). *Maintenance of Process Instrumentation in Nuclear Power Plants*. Berlin, Heidelberg: Springer-Verlag.

Hashemian, H. M. (2011). *Measurement of Dynamic Temperature and Pressures in Nuclear Power Plants*. Canada: University of Western Ontario.

He, X., & Tong, J. (2006). *Some Considerations for Implementing Human Reliability Analysis for Advanced reactors*. ESERL.

Hollifield, B., & Habibi, E. (2010). *The Alarm Management Handbook*. Houston, TX: PAS.

Hollnagel, E. (1993). *Human reliability analysis: Context and control*. London, UK: Academic Press.

Hollnagel, E. (2004). *Barriers and accident prevention*. Ashgate Pub Ltd.

Hood, C., & Rothstein, H. et al. (2004). *The Government of Risk. Understanding Risk Regulation Regimes*. Oxford, UK: Oxford University Press.

Miller, D. W., et al. (2006). *Instrumentation, Controls, and Human-Machine InterfaceWscience and Technology Roadmap*. 5th NPIC&HMIT; ANS. Albuquerque, NM.

NUREG-0800. (2010). *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants. Chapter 7. Imstrumentation and control.* US Nuclear Regulatory Commission, Washington, DC).

NUREG/CR-7006. (2010). *Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems*. Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J. (2009). *Applying Human Performance Models to Designing and Evaluating Nuclear Power Plants: Review Guidance and Technical Basis*. Upton, NY: Brookhaven National Laboratory. doi:10.2172/1013435

Sheridan, T. B. (2002). *Humans and automation: System design and research issues*. New York, NY, USA: Wiley & Sons Inc.

Spellman, F. R., & Whiting, N. E. (1999). *Safety Engineering: Principles and Practices*. Rockville, Maryland: Government Institutes.

Tong, L. S., & Weisman, J. (1996). *Thermal Analysis of Pressurized Water Reactors* (3rd ed.). ANS.

KEY TERMS AND DEFINITIONS

Component: A discrete element of a system. A component may be hardware or software and may be subdivided into other components. Examples are wires, transistors, integrate circuits, motors, relays, solenoids.

Equipment Family: A set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). An equipment family usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software.

Human-Machine Interface (HMI): The interface between operating staff and I&C system and computer systems linked with plant. The interface includes displays, controls, and the operator support system interface.

Individual I&C Systems: Systems together performing all I&C functions provided for overall I&C system, interacting with each other, with operating personnel and technological systems and equipment.

Instrumentation and Control System: A system, based on electrical and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself. The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices.

Overall I&C System: A system providing monitoring and control of all technological systems and equipment at NPP or individual NPP power generating unit.

Software-Hardware Complex (SHC): Functionally complete item in the form of one or several independently operated devices with built-in software, which are interconnected through electric and/or optic cables, with peripheral equipment of the same system and with other I&C systems. SHC is usually supplied to customer as a set with necessary service equipment, repair- and recovery reserve, operating and software documentation.

Chapter 2
International Standard Bases and Safety Classification

Michael Yastrebenetsky
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Grygoriy Gromov
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

ABSTRACT

The main standard bases for NPP I&C systems are documents of the International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC). Standards are interconnected through the following: IAEA develops general safety principles for NPP I&C systems, and IEC develops technical requirements that use and specify safety principles. Structures of the bases are considered. Classifications of I&C systems and their components are given on the basis of their safety impact. According to the IAEA classification, all systems are divided into safety important and non-safety important. According to IEC, functions to be performed by I&C systems shall be assigned to categories according to their importance to safety. The importance to safety of a function shall be identified by means of the consequences in the event of its failure, when it is required to be performed, and by the consequences in the event of a spurious actuation. All functions are divided into categories A, B, C.

INTRODUCTION

There is an expression that safety regulations are written with blood. It applies foremost to standards in nuclear power engineering, where accidents have a large-scale effect.

Standardization in nuclear power engineering, including NPP I&C systems, has specific peculiarities in comparison with other branches of industry.

Firstly, in nuclear power engineering there is a strict prohibition on any actions that are not specified by the regulations: those actions are forbidden that are not allowed. In many other branches of industry there is a reverse statement: those actions are allowed that are not forbidden. Allowed actions are described in standards as NPP safety in general, and NPP I&C that provides the safety, in particular.

Secondly, in consideration with a global scale of accident international cooperation is used extensively in nuclear power engineering. It applies to development and use of NPP I&C safety standards. Standard bases of the International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC) are the most widespread

DOI: 10.4018/978-1-4666-5133-3.ch002

in the world. These standards concentrate the best international experience of development and operation of NPP I&C. It is especially important for the countries that have less experience of using NPP and, in particular, NPP I&C. Our chapter is devoted to the description these standard bases, especially classification of I&C systems and their safety components.

Thirdly, there are particular aims of standards for nuclear I&C – to increase the confidence of the public with more stringent requirements than those typically applied to conventional industry standards, to verify and demonstrate the quality and reliability of the safety systems before NPP operation, to create international consensus among participating countries, operators, and vendors.

Note that besides international standards each country has a standard base concerning nuclear power engineering, including NPP I&C, e.g. American National Standards Institute (ANSI) in USA, Deutsches Institut fur Normung (DIN) in Germany, British Standards Institute (BSI) in UK). In addition, USA standards of professional organizations are widespread – American Society of Mechanical Engineering (ASME) and, especially concerning NPP I&C, – Institute of Electrical and Electronic Engineers (IEEE).

However, the main attention in this chapter is further given not to national, but to international standards, since harmonization of national standards with ones is currently a vital task.

BACKGROUND

Elaboration of international standards related to NPP I&C began immediately after commissioning of the first NPP. The International Electrotechnical Commission (IEC) created a separate technical committee devoted to NPP I&C, with name "Nuclear Instrumentation" in 1960. One of the first IEC publications-"General principles of nuclear reactor instrumentation" was issued in 1967. IEC understood importance of computer technique for NPP automatics: publication "Application of digital computer to nuclear reactor instrumentation and control "dates back to 1979.Computers only began to make first steps for their using at NPP at that time.

During more than 50 years IEC developed a lot of standards applicable to different types of I&C, to different aspects of NPP I&C design and operation. Special attention is paid to application of computer systems and the latest achievement in information technology.

The International Atomic Energy Agency (IAEA) elaborated Codes on safety of NPPs, which related to all NPP systems, including I&C (e.g., "50-C-D. Code on Safety on Nuclear Power Plants. Design" -1979). Special safety guides related exclusively to NPP I&C ("50-SG-D3. Protection Systems and Related Features in Nuclear Power Plants"- 1980). IEC and IAEA have close connections in the development of standard base for NPP I&C.

Many countries where NPPs are operated developed their national standard base related to I&C. One of the first American National Standards (based on IEEE Standard 323-1974) was ANSI/IEEE Std.323-1983 "IEEE Standard for Qualifying Class1 Equipment for Nuclear Power Generating Stations" which did not lose its importance for long time. The first USSR Regulation PBYa- 04-74 "Rules of NPP Nuclear Safety" which contained requirements on reactor control and protection systems, was issued in 1974.

Ukraine after gaining independence (1991) used to 1999 USSR regulations and standards related to NPP I&C. Ukrainian regulation "NP 306.5.02/3.035-2000. Requirements for nuclear and radiation safety information and control systems important to safety of nuclear power plants" was issued in 2000.

IAEA STANDARD BASE

The International Atomic Energy Agency (IAEA), created in Vienna in 1957, is an international intergovernmental organization bound with the Agreement with United Nations Organization (UN). The agreement stipulates that IAEA acts as an autonomous international organization, being in working relations with UN.

The objectives of the Agency are determined in its statute: "Article II: Objectives. The Agency shall seek to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world. It shall ensure, so far as it is able, that assistance provided by it or at its request or under its supervision or control is not used in such a way as to further any military purpose" (IAEA, 2013,b).

IAEA activities consist in providing emergency intervention in case of accidents, technical cooperation, information exchange, personnel training, and also in development of IAEA safety documents.

IAEA Safety Standards Series

According to the statute, IAEA determines safety standards and provides for their application. IAEA standards reflect the best experience and practices of countries, using nuclear power, and, as one of the main tasks, are intended to support formation of a proper national normative base.

From a legal point of view, IAEA standards are not mandatory for IAEA member countries, but can be adopted by their own choice.

IAEA safety standards were always combined by a certain family. Skipping a family of the standards that had been acting till 1996, let us mention that some of them were of direct relevance to NPP I&C:

- **IAEA 50-C-D:** Basic document of IAEA on NPP design (IAEA, 1988).
- **IAEA-50-SG-D3:** Document, containing requirements for protection systems and other control systems (IAEA, 1980).
- **IAEA 50-SG-D8:** Document, containing requirements for I&C important to safety, but not included in protection systems (IAEA, 1984).

These document played a significant role in NPP I&C development in different countries.

Since 1996 the system of standards has been replaced by IAEA Safety Standards Series. Standards of the series "Nuclear Safety" included three groups that were applied to NPP I&C:

- **"Safety Fundamentals":** Setting main objectives, concepts and principles of safety assurance.
- **"Safety Requirements":** Setting requirements that must be met for safety assurance. They are expressed in imperative form and defined by objectives and principles represented in "Safety Fundamentals."
- **"Safety Guides":** Containing recommendations based on international experience. These documents are less formal than "Safety Requirements" and specify actions, conditions and procedures to be complied with safety requirements.

Besides the group classification, standards are divided by topics: "NPP Design;" "NPP Operation."

By topic "NPP Design" and in group "Safety Requirements" let us note IAEA NS-R-1 "Safety of nuclear power plants: design. Safety requirements" (IAEA, 2000,a) that contains a separate section with I&C requirements, and also a set of provisions common for various NPP systems: objectives and concepts of safety; safety management requirements; general technical requirements; design requirements.

In group "Safety Guides" the standard IAEA NS-G-1.3 "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants" (IAEA, 2002) was issued in 2002. This document evolves provisions of IAEA NS-R-1(IAEA, 2000). In IAEA NS-G-1.3 various I&C systems important to safety are considered, including I&C with the use of programmable computers with frames of considered systems – from a sensor to an actuator inclusive. New document material is included in the overall process of I&C system design, in the processes of verification, validation, and documentation, and in the integration of human factors, and in the use of digital technology in I&C systems important to safety. Harmonization with proper international standards was improved (including IEC). IAEA NS-G-1.3 was compiled by leading experts of I&C of different countries (USA, Germany, Great Britain and others) and is one of the main IAEA documents on I&C important to safety. This document has determined paths of NPP I&C development for range of years.

Contents of IAEA NS-G-1.3:

1. Introduction.
2. Instrumentation and control systems important to safety.
3. The design basis.
4. General design guidelines (set of common requirements to I&C systems).
5. System specific design guidelines (protection systems, power supplies, digital computer systems, etc).
6. Human-machine interface.
7. Design process for I&C systems important to safety, etc.

Another IAEA standard, included in "Safety Guides" group and related to I&C, is IAEA NS-G-1.1 "Software for computer based systems important to safety in nuclear power plants" (IAEA, 2000,b). This standard is used together with IAEA NS-G-1.3 and contains the following sections:

1. Introduction.
2. Technical considerations for computer based systems.
3. Application of requirements for management of safety to computer based systems.
4. Project planning.
5. Computer system requirements.
6. Computer system design.
7. Software requirements.
8. Software design.
9. Software implementation.
10. Verification and analysis.
11. Computer system integration.
12. Validation of computer systems.
13. Installation and commissioning.
14. Operation.
15. Post-delivery modifications.

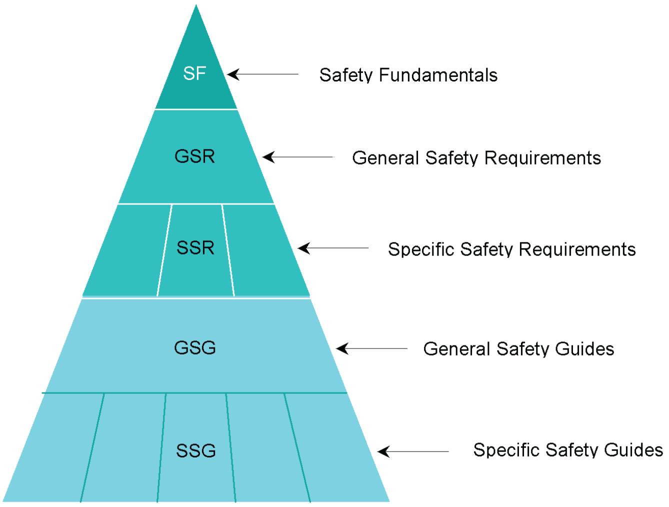
Since 2009 a new structure of IAEA standards has started operating. These standards have three categories (see Figure1).

"Safety Fundamentals": SF-1 "Fundamental Safety Principles" (IAEA, 2006) presents the fundamental safety objective and principles of protection and safety and provides the basis for the safety requirements.

"Safety Requirements": An integrated and consistent set of safety requirements establish the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements are governed by the objective and principles of the safety fundamentals. If the requirements are not met, measures must be taken to reach or restore the required level of safety. The format and style of the requirements facilitate their use for the establishment, in a harmonized manner, of a national regulatory framework.

The General Safety Requirements (GSR) are applicable to all facilities and activities. The

Figure 1. IAEA safety standards categories



examples are the documents (IAEA, 2010) and (IAEA, 2009).The Specific Safety Requirements (SSR) are applicable to specific installations and activities.

Overarching requirements of NPP I&C systems contain documents from group 2 “Specific safety requirements, devoted to safety of nuclear power plants”: “2.1 Design “(IAEA, 2012) and 2.2 “Commissioning and operation” (IAEA, 2011,a).

“Safety Guides”: Safety Guides provide recommendations and guidance on how to comply with the safety requirements, indicating an international consensus that is necessary to take the measures recommended (or equivalent alternative measures). The Safety Guides present international good practices, and increasingly they reflect best practices, to help users striving to achieve high levels of safety.

General Safety Guides (GSG) are applicable to all facilities and activities. Document number 1 of this group, GSG-1, is the guide, devoted to classification of radioactive waste, the second GSG-2 contains criteria for use in preparedness and response for a nuclear and radiological emergency.

Specific Safety Guides (SSG) are applicable to specified facilities or activities. The recently developed new safety guide “Design of I&C Systems for Nuclear Power Plants” (IAEA, 2013,a) will be related to Specific Safety Guide group. This document will combine and supersede the current 2 safety guides: NS-G-1.1 (IAEA, 2000, b) and NS-G-1.3 (IAEA, 2002).

Other IAEA Documents

International Nuclear Safety Advisory Group – INSAG, in which the most authoritative experts from different countries are working, was established in 1985. The group develops general safety concepts on the basis of analysis of activity results both within IAEA framework and on other information. INSAG documents formally have information status. However, in fact they should be applied in international practice, because they reflect international trends of nuclear safety and due to them documents of both IAEA and its member countries are issued. The first INSAG paper was devoted to causes and effects of the Chernobyl NPP disaster. For NPP I&C 75-INSAG-3 “Basic safety principles for nuclear power plants” is very important. It was issued in 1988, then revised in 1999 and reissued under the same title but with another number INSAG-12 (IAEA, 1999,a). The document contains objectives and fundamental principles of safety assurance.

Documents in IAEA Safety Report series –SRS contain papers made by of a group of experts, representing information publications without setting requirements. These publications describe practical experience, give practical examples and detail methods, used to achieve safety requirements compliance.

In IAEA Technical Report Series -TRS let us note a NPP I&C reference book (IAEA, 1999, b) prepared by a group of authors from different countries. A significant part of the book is occupied by a description of NPP I&C in Finland (Loviisa), France (series N°4), Great Britain (Sizewell B), Canada (CANDU, series 6), Russia (WWER-1000), USA and others. .Another example of a document of this series is a report on verification and validation of I&C software (IAEA, 1999, c).

A significant number of documents, related to NPP I&C, was issued in "*TECDOC*" series. These documents are generally devoted to specific tasks and summarize experience of IAEA member countries. The following issues are considered:

- Modernization and new technologies, including: software issues (quality assurance, verification and validation, life cycle management and others); digital hardware (reliability, safety analysis, I&C computerized hardware and others).
- Ageing and operating experience.
- Human factor, including operator support systems, man-machine interface, simulators and others.

An example of document in TECDOC series is IAEA-TECDOC-1016 "Modernization of instrumentation and control in nuclear power plants" (IAEA 1998), issued under the guidance of W. Bastl (Germany) and J. Naser (USA). It contains information about management of modernization, design criteria, requirements and restrictions, operating and licensing aspects, tests and also examples of I&C modernization in different countries – Hungary, German, Korea, Russia, USA, Finland, Czech Republic, Ukraine.

In the development of TECDOC documents a significant role was played by the Technical Working Group on NPP Instrumentation and Control, uniting experts from a number of countries. This group was created in 1970. The main objective of the Working Group is to promote the exchange of information on NPP I&C and to stimulate and, if possible, coordinate research in this field of NPP I&C in interested Member States and international organizations. The scope of work covers all aspects of the life cycle of I&C systems and equipment from feasibility study and design through installation, commissioning and licensing to operation, maintenance and decommissioning. The work thus not only covers technical details of the technology but also the management processes by which it is to be developed, designed, licensed, qualified installed, and maintained. In 2011 a report (IAEA, 2011,a) was prepared by the experts of this group, which is an introductory description of I&C systems and their life cycle. It compiles the necessary basic information to understand I&C systems in NPPs, an explanation of the significant role of I&C systems in maintaining and improving safety, plant performance, and economic.

IAEA SAFETY CLASSIFICATION PRINCIPLES

Safety class is an attribute that is taken into account by hardware and software developers, system designers, operating organization, other participants in I&C creation (modernization), nuclear regulatory authorities. One follows safety class in setting requirements on I&C systems and their components, developing, producing, product testing, designing, checking and providing maintenance, and also during assessment of their compliance with regulatory requirements.

It should be taken into account that a degree of "rigidity" of regulatory requirements depends considerably on a type of class, to which an object of standardization and safety assessment is referred.

Standards IAEA NS-R-1 (IAEA, 2000,a) and IAEA SSR-2/1 (IAEA,2012), covering not only the I&C, but also various NPP systems, determines that all items (i.e. systems, structures and components) important to safety, shall be identified and shall be classified on the basis of their functions and their safety significance. The method for classifying the safety significance shall be based primarily on deterministic methodologies complemented where appropriate by probabilistic methods, with account taken of factors such as:

- The safety function to be performed.
- The consequences of failure to perform the safety function.
- The frequency with which the item will be called upon to perform a safety function.
- The time following a postulated initiating event at which, or the period for which, it will be called upon to operate.

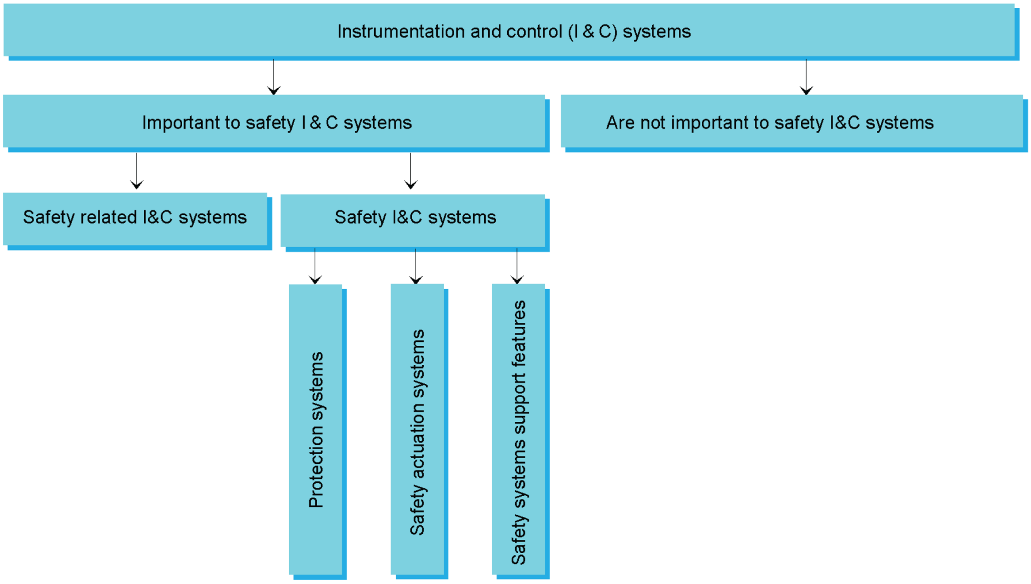
IAEA NS-G-1.3 (IAEA, 2002) expands the principle of classification to all I&C functions, systems, and components to fit into one of two safety categories: *important to safety or not important to safety* (Figure2). Functions, systems, and components important to safety are those whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public.

Functions, systems, and components important to safety are further categorized as either *safety* or *safety related*.

Safety functions, systems, and components are those provided to ensure the safe shutdown of the reactor, the residual heat removal from the core, control of reactivity, control of planned radioactive release, limitation of the consequences of anticipated operational occurrences or design basis accidents.

I&C safety systems initiate actuation and control actions of technological systems, performing emergency reactor trip, emergency core cooling, emergency containment isolation and others.

Figure 2. IAEA safety classification of I&C systems


Instrumentation and control (I & C) systems
Important to safety I & C systems
Are not important to safety I&C systems
Safety related I&C systems
Safety I&C systems
Protection systems
Safety actuation systems
Safety systems support features

Safety systems have been divided into the groups, which shown in Figure2.

1. Protection systems, which initiate I&C for:
   a. Reactor trip.
   b. Emergency core cooling.
   c. Decay heat removal.
   d. Containment isolation.
   e. Containment spray.
   f. Containment heat removal.
2. Safety actuation systems, which actuate I&C for:
   a. Reactor trip.
   b. Emergency core cooling.
   c. Decay heat removal.
   d. Confinement isolation.
   e. Containment spray.
   f. Containment heat removal.
3. Safety systems support features:
   a. Emergency power supply.
   b. Control room habitability.
   c. Safety equipment heating and cooling.

Safety related I&C systems are I&C systems important to safety that perform other functions important to safety which are not performed by I&C safety systems.

Examples of safety related systems are:

- Reactor control systems.
- Plant control systems.
- I&C control room.
- I&C fire detection and extinguishing.
- Radiation monitoring.
- Emergency control center.
- Communication equipment.
- I&C fuel handling and storage.
- I&C associated with the operation of the safety system.
- I&C for monitoring the state of the safety system.
- Access control systems.

INTERNATIONAL ELECTROTECHNICAL COMMISSION STANDARD BASE

IEC Standards Related Directly to NPP I&C

International Electrotechnical Commission (IEC) was founded in 1906 in order to facilitate international cooperation in the field of electrical and communication technology. Afterwards IEC sphere of activity was extended by electronics, instrument engineering, computers and other branches of modern technology, connected with information technologies. IEC is the oldest international organization of standardization. As of 2011, IEC members are represented by 81 countries. IEC member countries cover 80% of the world population and produce more than 95% of world electric energy. IEC is the biggest and the most authoritative organization of standardization in the world, covering a wide range of issues such as electrical engineering, electronics, instrument engineering, and computer technology.

IEC standardization covers two main aspects:

- The interchangeability of products.
- Standard methods of measuring and assessing quality and performance.

More information on IEC activity can be found at http:\www.iec.ch. IEC work is organized among technical committees (TC), and each TC is responsible for a specific course. Many of technical committees contains of subcommittees (SC), which in turn are divided in a range of Working Groups (WG) (Bouard, 2002; Cox&Shumov, 2011).

The subject of the book corresponds foremost to activities of TC 45 (Nuclear Instrumentation) and, in particular, to its subcommittee SC 45A (I&C of nuclear facilities). This subcommittee was formed in 1963 and is concerned with electronic and electrical functions and associated systems and equipment used in the instrumentation and control systems important to safety of nuclear power plants.

SC45A standards cover the entire lifecycle of these I&C systems, from conception, through design, manufacture, test, installation, commissioning, operation, maintenance, aging management, modernization and decommissioning.

A major aspect of SC45A is the application of emerging electronic techniques in order to meet nuclear instrumentation and control requirements, particularly computer systems and advances in information processing and control.

SC-45A now has 7 active Working Groups:

- **WG A2:** Sensors and measurement technique.
- **WG A3:** Application of digital processors to safety in NPPs.
- **WG A5:** Special process measurements and radiation monitoring.
- **WG A7:** Reliability of electrical equipment in reactor safety systems.
- **WG A8:** Control rooms.
- **WG A9:** Instrumentation systems.
- **WG A10:** Upgrading and modernization of I&C systems in NPPs.

The second subcommittee of technical committee TC-45 is SC45B (Radiation monitoring instrumentation).

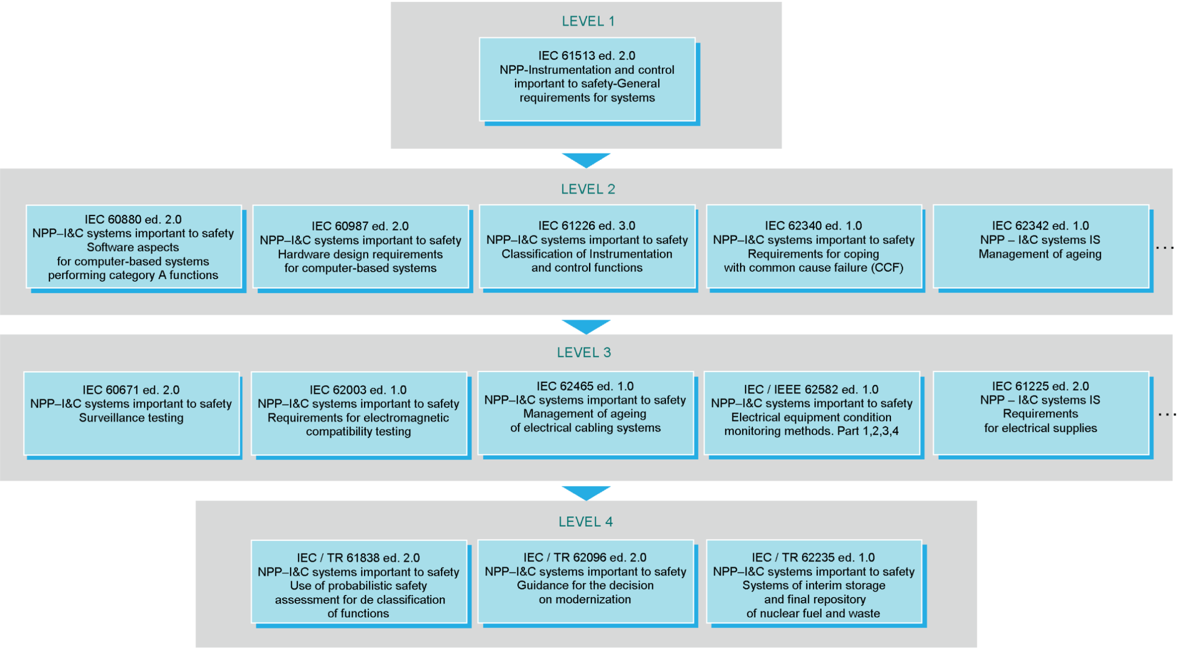
In Figure3 shows the structure of standards, developed SC45A and related to NPP I&C and its components important to safety, is n. Standards are arranged in 4 levels.

The top-level document is IEC 61513 (IEC, 2011,a). It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs.

IEC 61513 covers:

- Unit overall control systems and individual information and control systems.

Figure 3. Structure of IEC standards devoted to safety important NPP I&C systems and their components


LEVEL 1
IEC 61513 ed. 2.0
NPP-Instrumentation and control important to safety-General requirements for systems
LEVEL 2
IEC 60880 ed. 2.0
NPP–I&C systems important to safety Software aspects for computer-based systems performing category A functions
IEC 60987 ed. 2.0
NPP–I&C systems important to safety Hardware design requirements for computer-based systems
IEC 61226 ed. 3.0
NPP–I&C systems important to safety Classification of Instrumentation and control functions
IEC 62340 ed. 1.0
NPP–I&C systems important to safety Requirements for coping with common cause failure (CCF)
IEC 62342 ed. 1.0
NPP – I&C systems IS Management of ageing
...
LEVEL 3
IEC 60671 ed. 2.0
NPP–I&C systems important to safety Surveillance testing
IEC 62003 ed. 1.0
NPP–I&C systems important to safety Requirements for electromagnetic compatibility testing
IEC 62465 ed. 1.0
NPP–I&C systems important to safety Management of ageing of electrical cabling systems
IEC / IEEE 62582 ed. 1.0
NPP–I&C systems important to safety Electrical equipment condition monitoring methods. Part 1,2,3,4
IEC 61225 ed. 2.0
NPP – I&C systems IS Requirements for electrical supplies
...
LEVEL 4
IEC / TR 61838 ed. 2.0
NPP–I&C systems important to safety Use of probabilistic safety assessment for de classification of functions
IEC / TR 62096 ed. 2.0
NPP–I&C systems important to safety Guidance for the decision on modernization
IEC / TR 62235 ed. 1.0
NPP–I&C systems important to safety Systems of interim storage and final repository of nuclear fuel and waste

- Systems, using computers and software, and systems that do not use them.

In IEC 61513 two safety lifecycles are considered:

- Common, covering overall unit control systems.
- Individual information and control systems.

Common safety lifecycle follows from NPP safety design and includes:

- Operations prior to lifecycle of individual systems (e.g., architecture project of overall I&C systems).
- Lifecycles of individual I&C systems.
- Operations following the end lifecycle of individual systems (e.g., their integration).

The standard requires unambiguous, complete and clear functional requirements and design specifications, in relation to which functions should be checked during design, production, commissioning and maintenance, and which should be used as reference in performing any modifications.

System requirements in IEC 61513 are supplemented with requirements for system design, integration, validation, assembling, adjustment and operation, including requirements for their compliance assessment. Detailed documentation requirements at all stages of system lifecycle should be mentioned.

IEC 61513 contains description of a top level of requirements, regardless of reactor type and used design solutions: specification of a set of requirements contains in other IEC standards are at the 2-nd and 3-rd levels, as shown in Figure 3. IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defense against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513.

At the third level, IEC SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods, or specific activities.

At the fourth level technical reports, not considering normative documents, are found. There is only one document – IEC 61838 (IEC, 2001), devoted to the use of probabilistic safety assessment for the classification.

In this structure two earlier developed standards, having a wider application than I&C, are not included, - they cover different electrical equipment of safety systems, it follows that they are applied to safety control systems. Both standards consider equipment qualification: IEC 60780 (IEC, 1998) and IEC 60980 (IEC, 1989)

Technical report IEC 62096 TR "Nuclear power plant Instrumentation and Control – Guidance for decision on modernization" applies to all NPP I&C systems, regardless to safety importance.

In IEC standards a considerable attention is paid to aging management of NPP I&C equipment (see, e.g., IEC 62342 (IEC,2007,a). This standard considers requirements for aging management and control, for I&C aging phenomena and for evaluation of aging; aging stresses; and internal intended function versus qualification, maintenance, test, and operating data etc. "On-line" and "in-site" state monitoring of peripheral equipment (sensors, transmitters etc.) for defining its aging and applying proper actions are considered here. For this purpose computer technology without equipment dismounting on place of its installation in the unit and new analyzing instruments (neural networks, artificial intelligence, pattern recognition and others) are used. Examples of testing and monitoring techniques for I&C aging management are:

- On-line calibration verification.
- On-line detection of venture fouling.
- In situ response time testing of pressure transmitters.
- On-line detection of clogging in impulse lines.
- Resistor temperature detector (RTD) and thermocouple cross calibration.
- Response time testing of RTDs and thermocouples.
- Testing of cables and connectors.

The outlined problem, being very important, will not be considered in this book. The readers, who are interested in this problem, besides IEC standards, should be addressed to H. Hashimian's books (1998, 2005, 2006).

IEC Standards on Critical Systems: Functional Safety

IEC 61508 "Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems" (IEC, 2008), developed by technical committee IEC SC 65 "Industrial process measurement, control and automation," applies to critical systems in different branches of industry. This standard refers to a wide class of systems, including the following types of components: electrical (E) (e.g., electromechanical devices), electronic (E) (e.g., nonprogrammable transistor devices), programmable (PE) (e.g., microprocessors, microcontrollers, logic controllers). In IEC 61508 these components are indicated as E/E/PE and respective systems as E/E/PE systems or E/E/PES.

The definition of "functional safety" is given in IEC 61508: it is a part of general safety, related to controlled equipment and to a system that controls it, that depends on a correct operation of E/E/PE system important to safety, on other technological systems important to safety and devices for decreasing external risk. This concept and methods of functional safety assessment and assurance are more widely used currently.

IEC 61508 is a base for a range of safety important branches of technique. Examples of E/E/PE are fire control systems, ship motion control systems, railway signaling systems, automatic safety loading crane indicators, and, of course, NPPI&C systems.

In the standard, the notion of safety lifecycle is introduced, it is an activity connected with implementation of safety related systems starting from the development of design concept till E/E/PE systems are not usable. IEC 61508 describes two types of requirements:

- General control system requirements.
- Individual (separate) system requirements.

The standard indicates typical stages of system lifecycle and considers safety requirements for each of the stages.

"Functional safety" is a special case of more general concept "safety" and is in line with "fire safety," "electrical safety" etc.

IEC 61508 requires that functional safety assessment is made for all parts of E/E/PE system at all lifecycle stages. This standard is a basic: it is not only used as an independent one in some branches of industry, but also forms a ground for development of branch standards. In IEC 61508 the main attention is paid to computer systems.

To develop IEC 61508, later IEC 61511 (IEC, 2003) was issued: "Functional safety – Safety instrumented systems for process industry sector," consisting of three parts:

- **61511-1:** Framework, definitions, system, hardware and software requirements.
- **61511-2:** Guidance for the application of IEC 61511-1.
- **61511-3:** Guidance for the determination of the required safety integrity levels (a degree of risk reduction, provided by the system, is understood).

IEC 61513 (IEC, 2011,a) uses main principles of functional safety of basic IEC 61508, applying I&C (Figure 4). The necessity in IEC 61513 development, having a more common standard IEC 61508 for critical systems of various purpose, is connected with the fact that IEC 61513 a set of peculiarities of NPP safety assurance is taken into account, e.g. already available hazard information, availability of deterministic approach to determine system importance in terms of safety and others.

It should be noted that in IEC 61508 uses the term "safety related system." However, in IEC 61513, devoted to NPP I&C, this term is interpreted as "safety important system" according to IAEA nomenclature (see, e.g., IAEA, 2000,a and IAEA, 2012).

Following IEC 61508, functional safety of an I&C system can be called as a part of "nuclear and radiation safety of NPP" that refers to I&C operating in common and NPP technological equipment and depends on the I&C system correct functioning.

"Functional safety" term is relatively a new one. This term conforms to the problem of interconnection between the I&C and NPP safety: just I&C function performance affects NPP safety. Thus, the expression "I&C functional safety requirement" is identical to a longer expression "I&C requirements, affecting NPP nuclear and radiation safety."

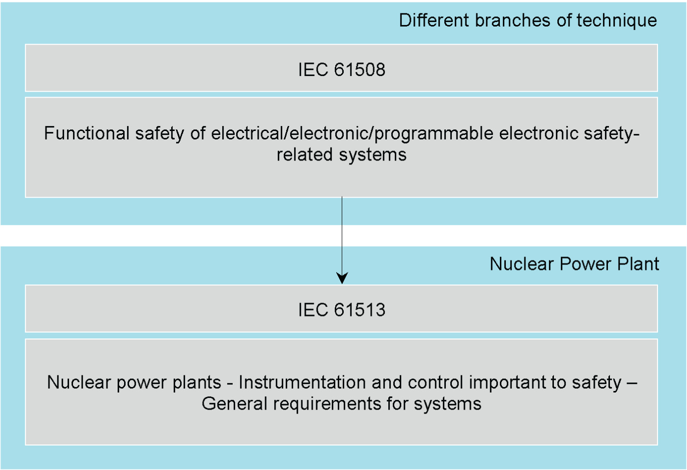
In Application D of IEC 61513 the interconnection between IEC 61508 and nuclear application standards is considered.

IEC Common Technical Standards

In IEC membership there is also a range of technical committees that developed common technical standards for different branches of technique, not only for NPPs. TC 77 "Electromagnetic compatibility" elaborated a set of standards with common name "Electromagnetic compatibility (EMC) – Testing and measurement techniques –" 61000-4- and additional name and number, which takes into account type of test (e. g. Electromagnetic compatibility (EMC) – Testing and measurement techniques – Electrostatic discharge immunity test IEC 61000-4-2).

The special importance of this group of standards is explained by the fact that advanced I&C

Figure 4. Relationship between IEC standards related to functional safety in different branches of technique and related to NPP I&C


Different branches of technique
IEC 61508
Functional safety of electrical/electronic/programmable electronic safety-related systems
Nuclear Power Plant
IEC 61513
Nuclear power plants - Instrumentation and control important to safety – General requirements for systems

systems use high-speed digital devices, communication networks, chips with high and extra high-scale integration (microprocessors, memory devices, programmable integrated logic circuits etc.) essentially sensitive to electromagnetic disturbances and power supply quality. Unexpected performance loss of individual components, caused by the interference or deviation of power supply parameters, can lead to unpredictable behavior of the whole system. IEC standards of 61000-4 series have considerably extended previous IEC ones.

Standards of technical committee IEC TC 56 “Dependability” have a great importance for NPP I&C. Dependability covers the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance (including management of obsolescence). The standards cover generic aspects on reliability and maintainability management, testing and analytical techniques, software and system dependability, life cycle costing, technical risk analysis and project risk management.

Let us also mention a standard issued by TC 75 on “Classification on environment conditions.”

Interconnection between IEC Standards and Other International Standards

IEC and IAEA closely interact with each other in the context of NPP I&C systems, though, their functions differentiate. According to a formal cooperation agreement between IAEA and TC 45 IEC, concluded in 1981, IAEA is responsible for development of general concepts for NPP I&C safety, TC-45 IEC is responsible for development of technical requirements, using and detailing the safety concepts mentioned above. Terms and definitions, used in IEC standards, correspond to IAEA standards.

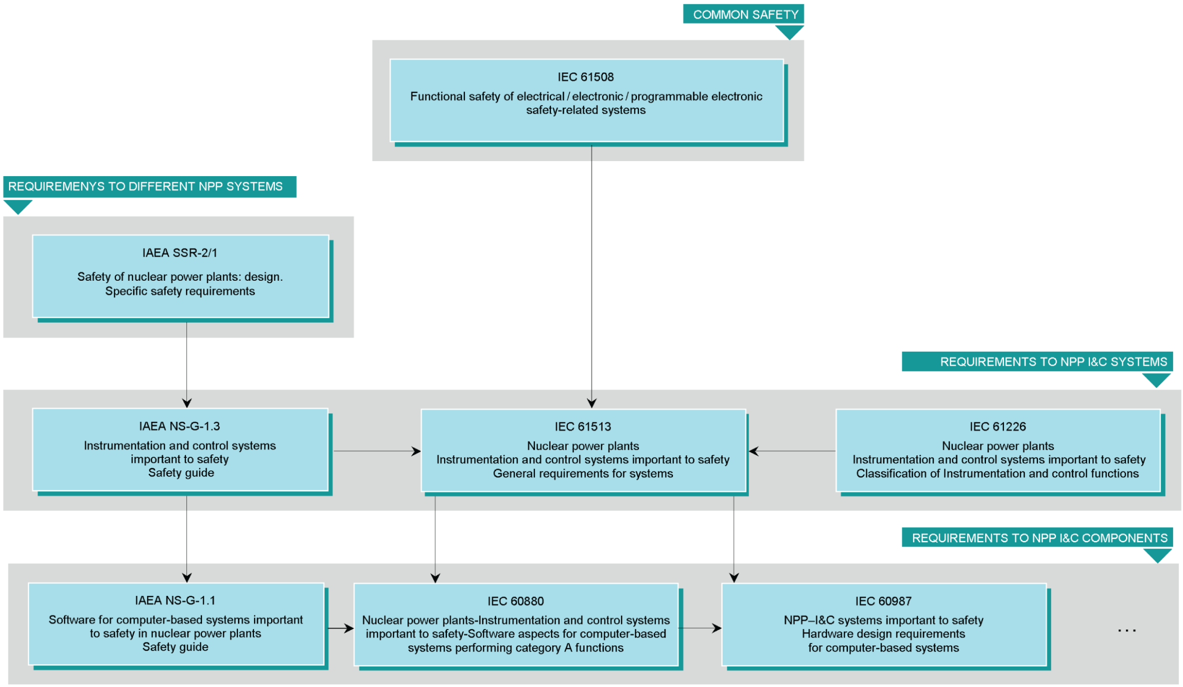
Interconnection between documents of IEC and IAEA is shown in Figure 5 that has a following structure. On the left IAEA documents are presented, on the right – IEC documents. The first level is general safety in different branches of industry, covered by IEC 61508, and IAEA documents are naturally not included. The second level is general NPP safety issues, covered by IAEA SSR-2/1, and IEC standards are not included. The third level is NPP I&C requirements and includes IAEA NS-G-1.3, subjected to IAEA NS-R-1 and corresponding to IEC 61513 and IEC 61226. The fourth level is I&C systems components. It includes IAEA NS-G-1.1 on NPP I&C software and IEC documents (e.g., IEC 60880 (IEC,2006) on software or IEC 60987 (IEC,2007,c). on computers.

At the regional level, the IEC works to achieve harmonization of standards among regional standardization organizations. A considerable part of European standards, developed by European Committee of Electrotechnical Standardization – CENELEC, is identical to IEC standards or slightly differs. So, all 7 parts of IEC 61508 are ratified by CENELEC, and this standard is published under EN 61508.

A number of IEC standards devoted to software (IEC, 2006, IEC, 2004,b), to hardware (IEC,2007,c), to classification of functions (IEC,2009,b), to control rooms (IEC,2009,a), to separation (IEC2004,a), to coping with common cause failures (IEC,2007,b), to data communication (IEC,2009,c), etc have been published as EN standards and implemented as nationally in 31 European countries.

IEC is closely connected with the International Organization for Standardization – ISO. In particular, taking into account rapid growth of computerization, in 1986 IEC and ISO created a joint technical committee (ISO/IEC Joint Technical Committee for Information Technology – JTC1). This committee consists of subcommittees. Standards applied in the field of NPP I&C are developed by subcommittee 7 on software engineering (JTC1/SC7 Software Engineering). A necessity of analysis of this group of standards is caused by a wide use of the latest achievements of information technologies in the I&C systems.

Figure 5. Interconnection between IAEA and I&C documents


COMMON SAFETY
IEC 61508
Functional safety of electrical / electronic / programmable electronic safety-related systems
REQUIREMENYS TO DIFFERENT NPP SYSTEMS
IAEA SSR-2/1
Safety of nuclear power plants: design. Specific safety requirements
REQUIREMENTS TO NPP I&C SYSTEMS
IAEA NS-G-1.3
Instrumentation and control systems important to safety
Safety guide
IEC 61513
Nuclear power plants
Instrumentation and control systems important to safety
General requirements for systems
IEC 61226
Nuclear power plants
Instrumentation and control systems important to safety
Classification of Instrumentation and control functions
REQUIREMENTS TO NPP I&C COMPONENTS
IAEA NS-G-1.1
Software for computer-based systems important to safety in nuclear power plants
Safety guide
IEC 60880
Nuclear power plants-Instrumentation and control systems important to safety-Software aspects for computer-based systems performing category A functions
IEC 60987
NPP–I&C systems important to safety
Hardware design requirements
for computer-based systems
...

The main part of standards on software engineering is devoted to the description of software (SW)lifecycle processes (supply and purchase, requirement analysis, design, coding and testing, integration, operation and maintenance, documentation, configuration management, quality assurance, verification and validation, project management). Moreover, a part of standards describe specific functions of software engineering: terminology development, specification of data and reports, measurement of SW characteristics, use and reuse of commercial products, application of instrumentation and formal methods.

IEEE standards form their own system inadequate to IEC standards. In particular, IEC focuses on important to safety systems, IEEE focuses on safety systems. It notes in (Johnson, 2002), that the collection of IEEE and IEC standards have some overlap, but in many cases cover significantly different topics. For example, IEEE standards go to great depth covering environmental qualification of many specific types of components, while IEC covers the topic only at the general level. Conversely, certain IEC standards deal with specific instrumentation and control functions, a topic area where IEEE standards are largely mute.

Collaboration between IEC with IEEE was realized as follow: two high level agreements signed in 2007 and 2008 between the IEC and the IEEE; technical collaboration started in 2009 between IEC/SC45A and IEEE/NPEC; publication of IEC/IEEE standards on condition monitoring took place in 2011 (IEC/IEEE, 2011). Drafts of new IEC/IEEE standards include:

- **Nuclear Power Plants:** Electrical equipment for safety systems- Qualification.
- **Nuclear Power Plants:** Control rooms- Computer based procedures.
- **New Direction of Common Work:** IEC/ IEEE standard, devoted to post-accident monitoring.

It may be supposed that this collaboration between IEC and IEEE will be considerably strengthened in the nearest future.

IEC SAFETY CLASSIFICATION PRINCIPLES

Categorization of Functions

IEC 61226 (IEC, 2009,b) defines a function is determined as a specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it. This standard extends the classification strategy presented in IAEA Safety Guide NS-G-1.3, and establishes the criteria and methods to be used to assign the I&C functions of an NPP to one of the three categories A, B and C, depending on their importance to safety, or to an unclassified category for functions.

Category A denotes the functions that play a principal role in the achievement or maintenance of NPP safety to prevent design basis event (DBE) from leading to unacceptable consequences. This role is essential at the beginning of the transient when no alternative actions can be taken, even if hidden faults can be detected. These functions play a principal role in the achievement or maintenance of the non-hazardous stable state.

Category B denotes functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the non-hazardous stable state has been achieved, to prevent DBE from leading to unacceptable consequences, or mitigate the consequences of DBE. The operation of a category B function may avoid the need to initiate a category A function.

Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Category C includes functions that have some safety significance, but are not category A or B. If a function does not meet any of the criteria given below, then it shall be “non-classified.”

IEC 61226 uses the approach based on qualitative criteria and not on probabilistic estimates (though, it indicates that probabilistic estimates can complete qualitative criteria). Most of the classification criteria are given in such a way that no additional analysis is required. For all categories examples of functions and systems, performing the functions, are given.

An I&C function shall be assigned to *category A* if it meets any of the following criteria:

- Functions required to reach the non-hazardous stable state, to prevent a DBE from leading to unacceptable consequences, or to mitigate its consequences.
- Functions, whose failure or spurious actuation would lead to unacceptable consequences, and for which no other category A function exists that prevents the unacceptable consequences.
- Functions required to provide information and control capabilities that allow specified manual actions necessary to reach the non-hazardous stable state.

The I&C functions assigned to category A are necessary for:

- Reactor shutdown and maintenance of sub-criticality.
- Isolation of containment.
- Provision of information for essential operator action.
- Decay heat transport the ultimate heat sink.

Typical I&C systems are as follows:

- Reactor protection system.
- Safety actuation system and safety support features.

- Key instrumentation and displays to permit pre-planned operator actions that are defined in the NPP operating instructions, and that are required to ensure NPP safety in the short term.

An I&C function shall be assigned to *category B* if it meets any of the following criteria and is not otherwise assigned to category A:

- Functions required after the non-hazardous stable state of a DBE has been reached, to prevent it from leading to unacceptable consequences, or to mitigate the consequences.
- Functions required to provide information or control capabilities that allow specified manual actions necessary after the non-hazardous stable state has been reached to prevent a DBE from leading to unacceptable consequences, or mitigate the consequences.
- Functions, the failure of which during normal operation, would require the operation of a category A function to prevent an accident which study is required.
- Functions to reduce considerably the frequency of a DBE as claimed in the safety analysis.
- Plant process control functions operating so that main process variables are maintained within the limits assumed in the safety analysis, when these control functions are the only means of control of these variables.
- Functions used to prevent or mitigate a radioactive release or fuel degradation outside of the limits and conditions of normal operation as defined in the safety analysis.
- Functions that provide continuous or intermittent tests or monitoring of functions in category A to indicate their continued availability for operation and alert control room staff to their failures, when no alternative means (e.g. periodic tests) are provided to verify their availability.

The I&C functions assigned to category B are necessary for:

- Used fuel pool cooling system.
- Main cooling system isolation.
- Post-accident monitoring system.
- Automatic control of the NPP primary and secondary circuit conditions, keeping variables in the limits assumed in the safety analysis, and prevention of events from escalating to accidents.
- Monitoring/controlling the handling of fuel where failure could cause radiation release or fuel degradation outside the limits and conditions of normal operation.

Typical I&C systems are as follows:

- NPP automatic control system or preventative protection system.
- Part of the decay heat transport to ultimate heat sink not necessary in the short term;
- Instrumentation needed to apply operating procedures for DBE.
- Safety circuits and interlocks of fuel handling systems used when the reactor is shut down.

An I&C function shall be assigned to *category C* if it meets any of the following criteria and is not otherwise assigned to category A or category B:

- Plant process control functions so that the main process variables are maintained within the limits assumed in the safety analysis and whose failure would not lead directly to operation of category A functions.

- Functions used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis.
- Functions that provide continuous or intermittent tests or monitoring of functions in category A and B to indicate their continued availability for operation and alert control room staff to their failures, and are not classified category B.
- Functions necessary to reach the safety probabilistic goals including those to reduce the expected frequency of a DBE.
- Functions to reduce the demands on a category A function, as claimed in the safety analysis;
- Functions to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood).
- Functions to warn personnel or to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure.
- Functions to monitor and take mitigating action following natural events (e.g. seismic disturbance, extreme wind etc).

The I&C functions assigned to category C include:

- Monitoring and controlling performance of individual systems and items of equipment during the post-accident phase to gain early warning of the onset of problems, and to keep radioactive releases ALARA.
- Limiting the consequences of internal hazards.
- Those for which operating mistakes could cause minor radioactive releases, or lead to radioactive hazard to the NPP operating staff.
- Those necessary to warn of internal or external hazard.
- Access control.
- Communication to warn of significant on- or off-site releases for the purposes of implementing the NPP's emergency plan.

Typical I&C systems are as follows:

- Alarm system.
- Access control system.
- Emergency communication systems.
- Control room data processing system.
- Fire suppression systems.

The first edition of IEC 61226 was issued in 1993. An offered classification proposed in the document at that time t seemed to be perspective, though a little exotic, since it did not correspond to the most part of NPP user countries. However, in following years this classification was more widely used. The very classification became basic for other IEC standards, devoted to NPP I&C important to safety. Thus, IEC 60880 (IEC 60880) describes software system requirements, performing category A functions.

Classification of Systems and their Components

According IEC 61513 (IEC, 2011,a), functions, systems and equipment of NPPs may be considered from two points of view: functionals or systems. Categorization of functions is shown hereinbefore.

From the second point of view, a system is classified (i.e. a total set of interconnection components, for which a composition, limits and a set of functions are specified). Each I&C important to safety should be classified according to categories of its functions, which are often related to different categories. IEC 61513 introduces a concept of system class and sets a relation between a category of function and minimum required I&C class that can perform this function (Table 1).

As it seen from the table, the standard provides division of system into three classes, unambiguously connecting them with three function catego-

Table 1. Correlation between classes of I&C systems and categories of I&C functions

Categories of I&C Functions Important to Safety			**Corresponding Classes of I&C Systems Important to Safety**
A	(B)	(C)	1
	B	(C)	2
		C	3

ries important to safety. Each class is characterized by a specific set of requirements for system features and capabilities, and also for design, production and quality of components. Satisfaction of these requirements allows considering a system as a proper one for performance of functions of a specific category. A system can perform or participate in performance of one or several functions of the highest category, corresponding to its class, and any number for functions of a lower category.

A typical classification of I&C systems is given in Table 2.

The requirements for the function with the highest safety category determine the class of the system.

Before classification of components notes that functions of I&C components (SHC, HW, and SW) are offered to be considered as components of those I&C functions, in performance of which they are participating. The classification of I&C systems component is based on the principle that each system function can be assigned to unambiguously specific set of components required and sufficient for realization of this function.

I&C safety class is reasonably set according to the following rules:

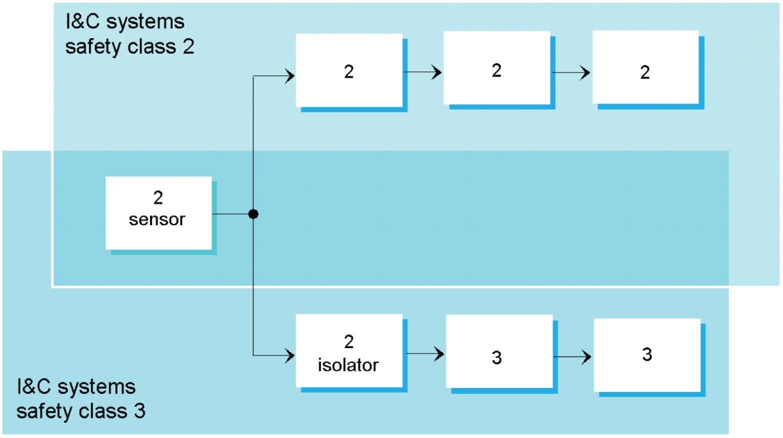
- Define a complete list of system functions, in realization of which this component is participating, and the category of each function.
- Refer all components that are participating in I&C function realization to the same category as this function.
- Determine component safety class, corresponding to the highest of the categories of these functions that it performs. Components that are participating in realization of one or several category A functions (and, possible, of other categories) are referred to the highest safety class.

If one component, for example, a sensor is included in several systems, it is referred to the highest of safety classes that it could have as a component of each of the systems separately (Figure 6). Hardware that is directly connected with components of a specific safety class is referred to the same class. An example could be signal galvanic isolation devices (also called "isolators"), providing a possibility to use the same sensors in the systems of different safety class, as shown in Figure 6. Communication lines, connecting components of one safety class, are referred to the same class; connecting components of different safety class — to the highest of the classes. The same rule is applied to equipment of data communication channels and local networks.

Table 2. Typical classification of I&C systems according to IEC

	Class 1	**Class 2**	**Class 3**	**Not Classified**
Plant automation and control systems		X	X	X
HMI systems (class 1 HMI may be restricted to a few critical indicators and push-buttons)	X	X	X	X
Protection system and safety actuation system	X			
Emergency power actuation system	X			

Figure 6. Safety classification of components, common for different I&C systems



2, 3 – safety classes of components

As an example in Figure7 shows a local network, through which data communication between I&Cs of 1 and 2 safety classes is performed. All components of such a local network, including data circuit terminating equipment (DCE), should be referred to the highest of safety classes (1), even in those cases when separate DCEs are included in systems of safety class 2. As in the previous example, in such systems special devices ("isolators") of safety class 1 should be provided to connect DCEs with components related to safety class 2.

Software safety class is set the same way as a safety class of instrumentation and control systems or HSC, with which this software is used.

Safety class of service items (including tools and service software) is proposed to install, taking into account:

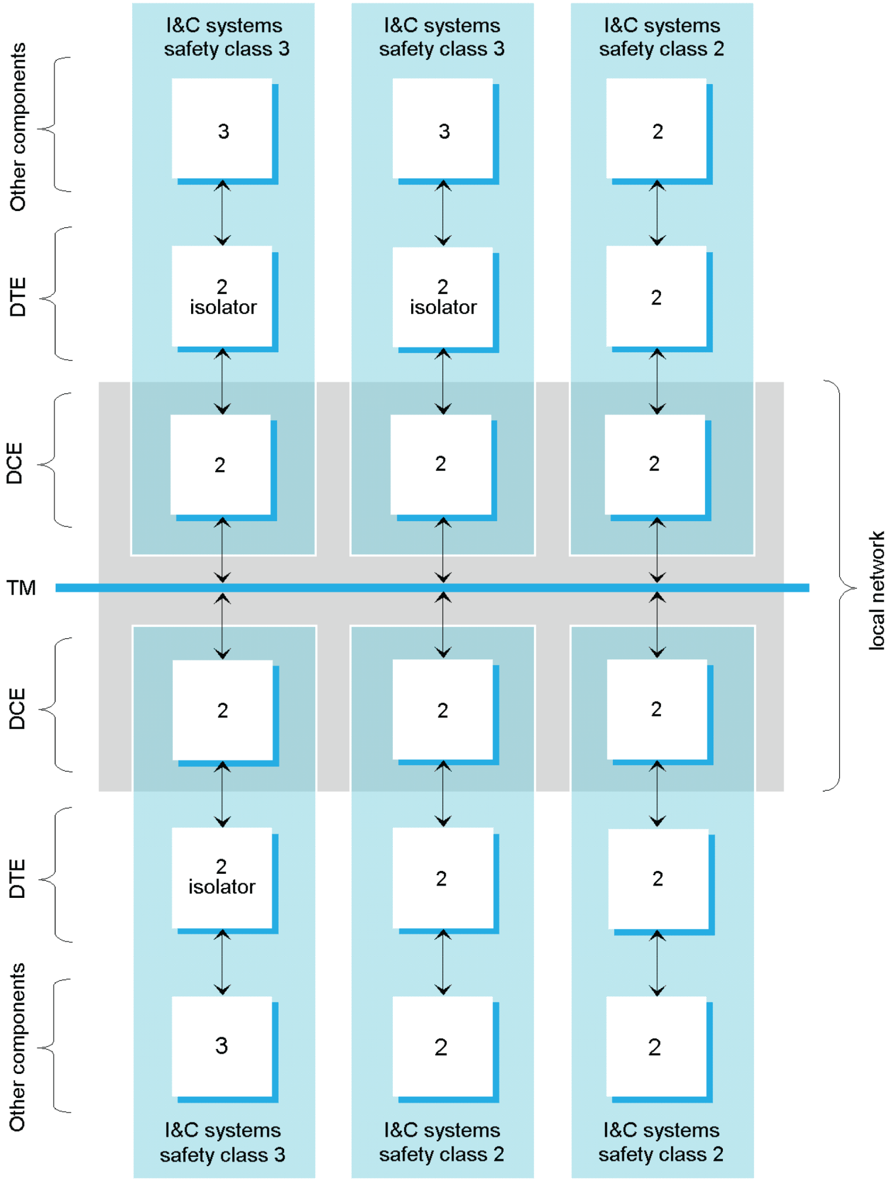
- Safety class of I&C, HSC and HW, in which the service Items included or with which service item is applied.
- Nature of performed service functions.
- Operation condition of I&C system, HSC or hardware while using service item as intended.
- Type of service item connection (permanent or only within a time period of its use as intended).

Safety class of service item, if permanently connected and allowing a direct influence on parameters and characteristics of I&C, SHC, HW or SW (change of modes, set-points, adjustments, installations or program modifications etc.), is identical to the safety class of system or component. In other cases the use of service items, related to a lower safety class, can be justified.

SAFETY CLASSIFICATION AND QUALITY REQUIREMENTS

To provide proper guarantee of operability and quality of I&C system operation, corresponding to their significance with regard to safety of systems and components of different classes, considerably distinct requirements should be applied. A general NPP safety concept is described in INSAG report (IAEA, 1999,a), where it is indicated that "all safety related components, structures and systems are classified on the basis of their functions and

Figure 7. Safety classification of a local network components



2, 3 – safety classes of components
DTE – Data Terminal Equipment
DCE – Data Circuit Terminating Equipment
TM – Transmission Medium

significance with regard to safety, and they are so designed, manufactured and installed that their quality is commensurate with that classification."

This concept is embodied in international standards. According to IAEA NS-G-1.3 "All I&C systems and equipment should be designed, constructed and maintained in such a way that their specification, verification and validation, quality assurance, quality control and reliability are commensurate with their classification." In the document requirements for all safety important systems and additional requirements related only to safety systems are provided. In particular, mandatory requirements for safety systems are: compliance with the single failure criterion; periodic checks and calibration of redundant channels for confirmation of specified operating characteristics; safety maintenance and no influence on other independent systems in testing. Analysis of probable common cause failures is required, and suitability of justified application of the diversity principle is indicated. Time minimization for redundant channel of safety system deactivation for checking is recommended, and safety requirements for testing equipment and facilities for its connection are set. For safety related systems these requirements are not regulated (or indicated as recommended).

IEC 61226 differentiates requirements for systems and equipment, depending on a category of the function they are performing. For each category general and specific requirements are determined. It is determined, for example, that reliability requirements can be identical for functions of different categories, though a level of confidence that the function will have the required reliability should be the highest for category A and can decrease for categories B and C. For category A functions redundancy, providing performance of, at least, the single failure criterion, should be applied. During reliability assessment common cause failure effects, which can be caused by defects of design, production, fitting or errors made by personnel during operation, servicing and restoration should be considered. If the specified factors cannot be taken into account, application of diversity means for function performance can be required.

For category B application of redundancy is desirable (but not mandatory if the required reliability level can be reached without redundancy). At the same time redundancy should be provided if single failure effects are not acceptable concerning a degree of their influence on safety. High reliability of component application should be justified. Application of means for fast detection and elimination of failures should be provided.

For category C in general case redundancy is not required, though it can be necessary for obtaining reliability level, in this case reliability and redundancy estimation should be assessed according to the same rules as for category B functions.

The requirements for functionality, environmental stability, tests, quality assurance which are differentiated for each safety category are determined in the same way.

It is obvious that an unreasonable setting a safety class of system and its components too high will cause a considerable increase of costs at all lifecycle stages: at development, validation, and verification of new hardware and software; production, equipment tests and acceptance; design, integration, checking, installation and commissioning; servicing and maintenance during operation. On the other hand, if systems (components) are related to a lower safety class, than is actually required, insufficiently strict requirements would be specified for them; in this case the quality of such systems (components) may not be complied with their actual significance with regard to safety and (or) a sufficient confidence in such compliance would not be obtained. Unreasonable understating of class should be considered as a hidden lack of safety, i.e. violation of one of the fundamental safety concepts.

SHORT REMARKS ON THE NATIONAL STANDARD BASES

Every country, where there are NPP's, has its own regulatory authority and own standard base related as to NPP safety as whole, as to NPP I&C systems.

Comparison of different I&C safety classifications is of interest is shown at Table 3 (the basis of this table is taken from (IAEA, 2011,b). In recent years after issuing of IEC 61226 and its following editions (let us note that besides IEC 61226 no IEC standards has been issued in a third revision over the recent 10 years) I&C systems division into 3 classes, corresponding to division of functions into 3 categories, is more widely applied. Harmonization with IEC 61226 is performed in the most part of European countries.

However, in Ukraine up to date safety important I&C systems have been divided into two safety classes (class 2 and 3). I&C systems were not related to class 1, according to high level document of regulatory authority of Ukraine,. Only now new regulations, where I&C systems are divided into 3 classes (Yastrebenetsky & Rozen, 2010), have been developed in Ukraine.

Though, it should be noted that the proposed I&C systems classification is not used, for example, in the USA, where only one safety class – 1E is determined. It includes electrical equipment and systems required for emergency reactor shutdown, isolation of containment, reactor core cooling, heat removal from containment and reactor or other actions important for prevention of radioactive materials into the environment (ANSI-IEEE). Other systems and equipment are not related to IE class.

At present, more attention is given to harmonization of international and national standards.

Solutions and Recommendations

International normative bases of IAEA and IEC are sufficiently coordinated and continue developing actively. New IEC standards and regular revisions of active ones, periodic redevelopment of IAEA documents prove these statements.

Two most important directions of work on standardization applicable to NPP I&C can be recommended:

1. Harmonization of national and international documents of different countries with international requirements.
2. Modification of requirements for NPP I&C, resulting from lessons of the Fukushima-1 accident. This recommendation will be considered below in Section "Future Research Directions" more detail.

FUTURE RESEARCH DIRECTIONS

The future research directions were pointed out in the paper of heads of IEC TC-45 (Cox & Shumov, 2010):

- Hardware, software and Commercial Off The Shelf (COTS) items are more and more used in instrumentation and control systems of nuclear reactors.
- Methods of information exchange (between instruments and control rooms, radio-links, exchange formats) are rapidly developing.
- The Internet impacts all industries and might need a specific approach for nuclear application.
- New types of reactors, such as advanced gas-cooled reactors, Pebble Bed Modular Reactors and reactors with higher power levels, are built in some countries. These types of reactors will require new types of instrumentation and control systems.

These trends either have already been taken into account in the project of international standards or they will be taken into account in the nearest future project."

Table 3. A comparison of different classifications of I&C systems

<table>
<tr><th>National or International Standard, Object of Classification</th><th colspan="7">Classification by the Importance to Safety</th></tr>
<tr><td rowspan="2">IAEA SSR-2/1,
IAEA NS-G-1.3, Systems</td><td colspan="6">Important to safety</td><td rowspan="2">Not
important to safety</td></tr>
<tr><td colspan="2">Safety</td><td colspan="4">Safety related</td></tr>
<tr><td>IEC 61226</td><td colspan="6">Important to safety</td><td></td></tr>
<tr><td rowspan="2">Functions</td><td colspan="2">Safety</td><td colspan="4">Safety related</td><td rowspan="2">No direct safety role
Unclassified</td></tr>
<tr><td>Category A</td><td colspan="3">Category B</td><td colspan="2">Category C</td></tr>
<tr><td>European utility requirements</td><td>F1A</td><td colspan="3">F1B</td><td colspan="2">F2</td><td>Unclassified</td></tr>
<tr><td>IEC 61513</td><td colspan="6">Important to safety</td><td rowspan="2">Not important to safety
Unclassified</td></tr>
<tr><td>Functions</td><td>Category A</td><td colspan="3">Category B</td><td colspan="2">Category C</td></tr>
<tr><td>Systems</td><td>Class 1</td><td colspan="3">Class 2</td><td colspan="2">Class 3</td><td>Unclassified</td></tr>
<tr><td>Germany</td><td colspan="6">Important to safety</td><td rowspan="3">Not important to safety
Unclassified
Unclassified</td></tr>
<tr><td rowspan="2">Functions
Systems</td><td>Category A</td><td colspan="3">Category B</td><td colspan="2">Category C</td></tr>
<tr><td>Class 1</td><td colspan="3">Class 2</td><td colspan="2">Class 3</td></tr>
<tr><td rowspan="3">United Kingdom
Function
Systems</td><td colspan="6">Important to safety</td><td rowspan="3">Not important to safety
Unclassified
Unclassified</td></tr>
<tr><td>Category A</td><td colspan="3">Category B</td><td colspan="2">Category C</td></tr>
<tr><td>Class 1</td><td colspan="3">Class 2</td><td colspan="2">Class 3</td></tr>
<tr><td>France N°4</td><td colspan="6">Important to safety</td><td>Not important to safety</td></tr>
<tr><td>Systems</td><td>1E</td><td colspan="3">2E</td><td>SH</td><td>Important to safety</td><td>-</td></tr>
<tr><td rowspan="2">Switzerland
Functions</td><td colspan="6">Important to safety</td><td rowspan="2">Not important to safety
Unclassified</td></tr>
<tr><td>Category A</td><td colspan="3">Category B</td><td colspan="2">Category C</td></tr>
<tr><td rowspan="3">Ukraine(draft of regulation)
Functions
Systems</td><td colspan="6">Important to safety</td><td rowspan="3">Not important to safety
Unclassified
Class 4</td></tr>
<tr><td>Category A</td><td colspan="3">Category B</td><td colspan="2">Category C</td></tr>
<tr><td>Class 2(A)</td><td colspan="3">Class 3(B)</td><td colspan="2">Class 3(C)</td></tr>
<tr><td rowspan="2">Ukraine(acting)
Systems</td><td colspan="6">Important to safety</td><td rowspan="2">Not important to safety
Class 4</td></tr>
<tr><td colspan="3">Class 2</td><td colspan="3">Class 3</td></tr>
<tr><td rowspan="3">Russia
Components
Functional groups</td><td colspan="6">Important to safety</td><td rowspan="3">Not important to safety
Class 4
Category K4</td></tr>
<tr><td colspan="3">Class 2</td><td colspan="3">Class 3</td></tr>
<tr><td>Category K1</td><td colspan="3">Category K2</td><td colspan="2">Category K3</td></tr>
<tr><td>Canada</td><td>Category1</td><td colspan="3">Category2</td><td colspan="2">Category3</td><td>Category4</td></tr>
<tr><td>Japan</td><td>PS1/MS1</td><td colspan="3">PS2/MS2</td><td colspan="2">PS3/MS3</td><td>Non-nuclear safety</td></tr>
<tr><td>Republic of Korea</td><td colspan="3">IC-1</td><td colspan="3">IC-2</td><td>IC-3</td></tr>
<tr><td rowspan="2">USA and IEEE</td><td colspan="6">Important to safety</td><td rowspan="2">Non-nuclear safety</td></tr>
<tr><td>Safety
Class 1E</td><td colspan="5">No name assigned</td></tr>
</table>

In addition new directions of work have appeared in relation to the Fukushima-1 accident.

Lessons of each major accident at NPPs include modification of standard bases of both international and national. These modifications were made after the TMI accident in the USA, Chernobyl accident in Ukraine, and now take place after Fukushima-1 accident in Japan. Modifications are applied to both general principles of nuclear safety and NPP I&C.

IAEA, IEC and national regulatory authorities began to change the requirements on NPP I&C after the accident at Fukushima-1 NPP. The main directions for standards development are the following:

- Elaboration of the concept of "hardened instrumentation" (sensors – in the first turn).
- Standard to cover spent fuel pool monitoring.
- Standard to cover containment monitoring.
- Standard to cover pressure transmitters specific to nuclear applications.
- Standard to cover seismic instrumentation: detection and measurement of the magnitude of the earthquake to help operators to analyze the possible consequences on the plant.
- Standard to cover boron concentration instrumentation.
- Standard to cover reactor pressure level instrumentation – characteristics and test methods.
- Standard to cover H2 instrumentation – characteristics and test methods.
- Standard to cover emergency response centre.

IEC did not have its own standards devoted to post- accident monitoring system. IEEE developed the first version of such standard after the TMI accident on in 1981, then also in 2002 and in 2010 revised it (IEEE, 2010). IEC decided not to develop own new standard on this subject, but to use IEEE experience and create a joint IEEE/ IEC standard. This work has started in 2012 by a group of experts from IEEE and IEC.

Note one of the interesting subjects for research directions- comparison of standards devoted to safety important/ safety related systems for different applications (e.g. Biscollio & Fusani, 2010)

CONCLUSION

The goals of standards, that pertain to NPP I&C systems, are:

- Establish requirements for I&C systems that are needed to assure NPP safety.
- Make available to designers sufficiently effective methods for elaboration of I&C systems and their components in accordance with the acting requirements.
- Establish methods for checking conformity of I&C systems with the requirements.
- Assure certain frameworks for interface between NPP plant, different participants of I&C systems development, and the regulatory body.
- Establish requirements for I&C systems operation.
- Establish terminology in the field of NPP I&C systems.
- Serve as a legal base in case of conflicts.

The International standard bases of International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC). related to NPP I&C systems, are described in this chapter. The IEC standard base is very advanced and includes more than 50 standards. These bases systematically are improved and supplemented. A great part of new additions concerns to new safety requirements after accident on Fukushima-1 .Of course, the development of international standard bases continues. The main position in IAEA standard base, related to NPP I&C, will rank IAEA safety standards "Design of Instrumentation and Control Systems for Nuclear Power Plants," which will supersedes IAEA standards NS-G-1.1 and NS-G-1.3.

Besides international standards, all countries used national ones. The harmonization of national and international standards is an urgent task.

Note that some of the standards in force in the United States(developed by the American Institute of Electrical and Electronics Engineers - IEEE, and the American Society of Mechanical Engineers -- ASME and others) de facto have become international standards and have been widely adopted not only in the United States but in other countries, successfully supplementing the IEC standards. This, for example, pertains to standards on qualification of equipment, to post-accident monitoring, etc. The main distinction, however, is the fact that the IEEE standards focus on safety systems, and the IEC standards focus on systems that are important for safety.

Many documents of the U.S. Nuclear Regulatory Commission (U.S.NRC) have received international use. An example of a U.S.NRC document which has been widely disseminated is NUREG-0800, which contains standard plans for safety analysis of different structures, components, equipment and systems. Section 7.0 of this document is devoted to I&C systems.

REFERENCES

Biscoglio, I., & Fusani, M. (2010). Analyzing quality aspects in safety-related standards. In *Proceedings of Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010*. Las Vegas, NV: American Nuclear Society.

Bouard, J.-P. (2002). International standardization in nuclear I&C engineering. In *Proceedings of CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems*. AEN/NEA.

Cox, M., & Shumov, S. (2011). About activities of IEC/TC45 nuclear instrumentation. *Nuclear Measurement and Information Technologies, 3*(35).

Hashemian, H. (2006). *Maintenance of process instrumentation in nuclear power plants*. Berlin: Springer.

Hashemian, H. M. (2005). *Sensor performance and reliability*. Research Triangle Park, NC: The Instrumentation, Systems and Automation Society.

Hashemian, H. M. et al. (1998). *Advanced instrumentation and maintenance technologies for nuclear power plants (NUREG/CR-5501)*. Washington, DC: U.S. Nuclear Regulatory Commission.

Hughes, P. J., & Johnson, G. L. (2000). Instrumentation and control systems important to safety: A new IAEA safety guide. *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies* (NPIC&HMIT 2000). Washington, DC: NPIC & HMIT.

IAEA. (1980). 50-SG-D3. *Protection systems and related features in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1984). 50-SG-D8. *Safety related instrumentation and control systems for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1988). 50-C-D. *Code on the safety on nuclear power plants: Design*. Vienna, Austria: IAEA.

IAEA. (1998). TECDOC-1016. *Modernization of instrumentation and control in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1999a). INSAG-12. *Basic safety principles for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1999b). *Modern instrumentation and control for nuclear power plants: A guidebook*. Vienna, Austria: IAEA.

IAEA. (1999c). *Verification and validation of software related to nuclear power plant instrumentation and control*. Vienna, Austria: IAEA.

IAEA. (2000a). NS-R-1. *Safety of nuclear power plants: Design: Safety requirements*. Vienna, Austria: IAEA.

IAEA. (2000b). NS-G-1.1. *Software for computer based systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2000c). NS-R-2. *Safety of nuclear power plants: Operation: Safety requirements*. Vienna, Austria: IAEA.

IAEA. (2002). NS-G-1.3. *Instrumentation and control systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2006). NS-G-1.3. *Fundamental safety principles*. Vienna, Austria: IAEA.

IAEA. (2009). *Safety assessment for facilities and activities: General safety requirements*. IAEA safety standards series No. GSR Part 4. Vienna, Austria: IAEA.

IAEA. (2010). *Governmental, legal and regulatory framework for safety: General safety requirements*. IAEA safety standards series No. GSR Part 1, Vienna, Austria: IAEA.

IAEA. (2011a). SSR-2/2. *Safety of nuclear power plants: commissioning and operation: Specific safety requirements*. Vienna, Austria: IAEA.

IAEA. (2011b). NP-T-3.12. *Core knowledge on instrumentation and control systems in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (2012). SSR-2/1. *Safety of nuclear power plants: design: Specific safety requirements*. Vienna, Austria: IAEA.

IAEA. (2013a). DS-431. (Draft safety guide). *Design of instrumentation and control systems for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (2013b). *The statute of the IAEA*. Retrieved from www.iaea.org/About/statute.html

IEC. (1980). IEC 60780. *Nuclear power plants – Electrical equipment of the safety system – Qualification*.

IEC. (1989). IEC 60980. *Recommended practices for seismic qualification of electrical equipment of the safety for nuclear generating stations*.

IEC. (2001). IEC 61838. *Nuclear power plants – Instrumentation and control functions important for safety – Use of probabilistic safety assessment for the classification*.

IEC. (2003). IEC 61511. *Functional safety – Safety instrumental systems for the process industry sector*.

IEC. (2004a). IEC 60709. *Nuclear power plants – Instrumentation and control systems important to safety – Separation*.

IEC. (2004b). IEC 62138. *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.*

IEC. (2006). IEC 60880. *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions.*

IEC. (2007a). IEC 62342. *Nuclear power plants – Instrumentation and control systems important to safety – Management of aging*.

IEC. (2007b). IEC 62340. *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF).*

IEC. (2007c). IEC 60987. *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems.*

IEC. (2008). IEC 61508. *Functional safety of electrical/electronic/programmable electronic safety-related systems*.

IEC. (2009a). IEC 60964. *Nuclear power plants – Control rooms – Design*.

IEC. (2009b). IEC 61226. *Nuclear power plants – Instrumentation and control important to safety–Classification of instrumentation and control functions*.

IEC. (2009c). IEC 61226. *Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category a functions*.

IEC. (2011a). IEC 61513. *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*.

IEC/IEEE. (2011). IEC/IEEE 62582. *Nuclear power plants – Instrumentation and control important to safety – Electrical equipment condition monitoring methods – Part 1: General: Part 2: Indenter modulus: Part 4: Oxidation induction techniques*.

IEEE. (2010). IEEE std. 497.2010. *IEEE standard criteria for accident monitoring instrumentation for nuclear power generating stations*.

Johnson, G. (2002). Comparison of IEC and IEEE standards for computer-based control systems important to safety. In *Proceedings of CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems*. AEN/NEA.

Yastrebenetsky, M., Rozen, Y., et al. (2010). Ukrainian NPP I&C standard base: Elaboration and application. In *Proceedings of Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010*. Las Vegas, NV: American Nuclear Society.

ADDITIONAL READING

IAEA. (1999, b). *Verification and validation of software related to nuclear power plant instrumentation and control.* Technical reports series Nº384. IAEA, Vienna.

IAEA. (1999, a). *Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook. Technical report series Nº387.* A Guidebook, IAEA, Vienna.

IAEA NP-T-1.1 (2008). *On-line Monitoring for Improving Performance of Nuclear Power Plants. Part 1: Instrument Channel Monitoring,* IAEA Vienna.

IAEA NP-T-1. 2 (2008). *IAEA, On-line Monitoring for Improving Performance of Nuclear Power Plants. Part 2: Process and Component Condition Monitoring and Diagnostics,* IAEA, Vienna.

IAEA NP-T-1. 3 (2008). *Role of I&C Systems in Power Uprating Projects in Nuclear Power Plants,* IAEA, Vienna.

IAEA NP-T-1. 4 (2008). *Implementing digital instrumentation and control systems in the modernization of nuclear power plants,* IAEA, Vienna.

IAEA NP-T-1. 5 (2009).Protecting Against Common Cause Failures in Digital I&C Systems, IAEA, Vienna.

IAEA NP-T-3. 10 (2010).*Integration of Analog and Digital Instrumentation and Control Systems in Hybrid Control Rooms,* IAEA, Vienna.

IAEA NP-T-3. 12 (2011).Core knowledge on instrumentation and control systems in nuclear power plants, IAEA, Vienna.

IAEA-TECDOC-1016 (1998).*Modernization of Instrumentation and Control in Nuclear Power Plants*, IAEA, Vienna.

IAEA-TECDOC-1066 (1999).*Specification of Requirements for Upgrades Using Digital Instrument and Control Systems*, IAEA, Vienna.

IAEA-TECDOC-1140 (2000).*Effective handling of software anomalies in computer based systems at NPPs*, IAEA, Vienna.

IAEA-TECDOC-1147 (2000).*Management of Ageing of I&C Equipment in Nuclear Power Plants*, IAEA, Vienna.

IAEA-TECDOC-1188 (2000).*Assessment and Management of Ageing of Major Nuclear Power Plant Components Important to Safety: In-Containment Instrumentation and Control Cables*, Vol 1 and 2, IAEA, Vienna.

IAEA-TECDOC-1197 (2001).*Assessment and management of ageing of major nuclear power plant components important to safety: CANDU reactor assemblies*, IAEA, Vienna.

IAEA-TECDOC-1252 (2001).*Information Integration in Control Rooms and Technical Offices in Nuclear Power Plants*, IAEA, Vienna.

IAEA-TECDOC-1284 (2002).*Information technology impact on nuclear power plant documentation*, IAEA, Vienna.

IAEA-TECDOC-1327 (2002).*Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants*, IAEA, Vienna.

IAEA-TECDOC-1328 (2002).*Solutions for cost effective assessment of software based instrumentation and control systems in nuclear power plants*, IAEA, Vienna.

IAEA-TECDOC-1389 (2004).*Managing Modernization of Nuclear Power Plant Instrumentation and Control Systems*, IAEA, Vienna.

IAEA-TECDOC-1402(2004).*Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance*, IAEA, Vienna.

IAEA-TECDOC-1500(2006).*Guidelines for Upgrade and Modernization of Nuclear Power Plant Training Simulators*, IAEA, Vienna.

IAEA-TECDOC-1544 (2007).*Nuclear Power Plant Design. Characteristics. Structure of Nuclear Power Plant Design Characteristics in the IAEA Power Reactor Information System (PRIS)*, IAEA, Vienna.

IAEA-TECDOC-1662 (2011).*Preparing and Conducting Review Missions of Instrumentation and Control Systems in Nuclear Power Plants*, IAEA, Vienna.

IAEA-TECDOC-448 (1988).*Analysis and Upgrade of Instrumentation and Control Systems for the Modernization of Research Reactors*, IAEA, Vienna.

IAEA-TECDOC-549 (1990).*Computer Based Aids for Operator Support in Nuclear Power Plants,* IAEA, Vienna.

IAEA-TECDOC-565 (1990).*Control rooms and man-machine interface in nuclear power plants*, IAEA, Vienna.

IAEA-TECDOC-581 (1991).*Safety implications of computerized process control in nuclear power plants,* IAEA, Vienna.

IAEA-TECDOC-668 (1992).*The Role of Automation and Humans in Nuclear Power Plants,* IAEA, Vienna.

IAEÂ-TECDOC-669. (1992). *Case study on the use of PSA methods: assessment of technical specifications for the reactor protection system instrumentation*. Vienna: IAEA.

IAEA-TECDOC-672 (1992).*Safety aspects of nuclear power plant automation and robotics*, IAEA, Vienna.

IAEA-TECDOC-762 (1994).*Operator support systems in nuclear power plants*, IAEA, Vienna.

IAEA-TECDOC-780 (1992). *Safety assessment of computerized control and protection systems*, IAEA, Vienna.

IAEA-TECDOC-790 (1993).*Reliability of computerized safety systems at nuclear power plants,* IAEA, Vienna.

IAEA-TECDOC-808 (1995).*Computerization of operation and maintenance for nuclear power plants*, IAEA, Vienna.

IAEA-TECDOC-812 (1995).*Control room systems design for nuclear power plants*, IAEA, Vienna.

IAEA-TECDOC-912 (1996).*Computerized support systems in nuclear power plants,* IAEA, Vienna.

IAEA-TECDOC-932 (1997).*Pilot study on the management of ageing of instrumentation and controls cables*, IAEA, Vienna.

IAEA-TECDOC-952 (1997).*Advanced control systems to improve nuclear power plant reliability and efficiency*, IAEA, Vienna.

IAEA-TECDOC-995 (1998).*Selection, specification, design and use of various nuclear power plant training simulators*, IAEA, Vienna.

IEEE 1289 (1998). IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations.

IEEE Std 1082 (1997). IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations.

IEEE Std 845 (1999). Guide for the Evaluation of Human-system Performance in Nuclear Power Generating Stations.

IEEE Std 379 (2000). Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.

IEEE Std 308 (2001). IEEE standard criteria for class 1E power systems for nuclear power generating stations.

IEEE Std 352 (2001). Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.

IEEE Std 323 (2003). Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 323 (2003). Qualifying Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 344 (2004). Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 577 (2004). IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities.

IEEE Std 1023 (2004). IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities.

IEEE Std 384 (2008). Standard Criteria for Independence of Class 1E Equipment and Circuits.

IEEE Std 603 (2009). IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

IEEE Std 7-4.3.2 (2010). Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

IEEE Std 627 (2010). IEEE Standard for Qualification of Equipment Used in Nuclear Facilities.

KEY TERMS AND DEFINITIONS

Functional Safety: Part of general safety which is determined by controlled equipment (a facility, plant, machinery) and system which controls ones.

Item Important to Safety: Item, whose failure or wrong operation can lead to violation.

Regulatory Requirement: A requirement which is established by the National Regulatory Authority (authority designated by government for regulatory purposes for safety assurance).

Safety Classification: Differentiation of systems or their components into classes, depending on their impact on NPP safety.

Safety Function: A specific purpose that have to be fulfilled for safety assurance.

Safety Fundamentals: A document which contains fundamental principles of safety assurance and safety objectives.

Standard Base: A set of standards or regulations which is established by government or international organizations for specific area of activity.

Chapter 3
Properties of Safety Important I&C Systems and their Components

Yuri Rozen
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

ABSTRACT

Operation reliability of NPP I&C and its components is considered in this chapter. Besides quantitative measures, qualitative features that provide required functional reliability such as protection against Common Cause Failures (CCF), single-failure criterion, redundancy, diversity, prevention of personnel errors, and technical diagnostics, are discussed. A group of features of NPP I&C and its components, united by "performance resistance," is also considered. In particular, they are resistance to environment influences, mechanical influences (including earthquake impacts), insensitivity changes of power supply, and electromagnetic disturbances. Operation quality issues are considered. By quality (in a broad sense), the authors mean the accuracy, response rate characteristics, and features of human-machine interfaces. Features that provide NPP I&C independence from malfunction or removal from operation of system components (including redundant ones) or from adjacent NPP I&C, and the decrease of possible impact of components on other adjacent systems (electromagnetic emission, fire safety) are described as well.

INTRODUCTION

The steadily growing role of up-to-date instrumentation and control (I&C) systems that assure NPP safety and security requires that:

- Properties of each I&C system and its components (hardware and software) at all life cycle stages should meet requirements of national and international regulations, rules and standards of nuclear safety.
- A procedure of development, design, manufacturing, testing, acceptance and operation of the system and its components determined by regulations, rules and standards of nuclear safety should be observed. for each I&C system.

IEC standard 61508 (IEC, 2008) interprets compliance with the indicated requirements as *functional safety* of I&C system.

DOI: 10.4018/978-1-4666-5133-3.ch003

The object of the chapter – is to show those general properties of I&C systems and their central equipment (software-hardware complex - SHC) and peripheral equipment, used during NPP automation, that provide functional safety of these systems.

BACKGROUND

Experience of international society in NPP safety assurance, including functional safety of I&C systems, accumulated in requirements of national and international regulations, rules and standards of nuclear safety and was considered during the large-scale modernization, carried out at all Ukrainian NPPs within programs of safety improvement and extension of service life of operating power units. These activities contributed to accumulation of Ukrainian own experience in standardization, assurance and assess of functional safety (further – safety) of I&C systems, implemented using up-to-date technologies, modern electronic components and computing technology, optic communication networks, computer facilities for diagnostic, display, archiving, etc.

The properties of safety important I&C systems and their components that are described further are determined by the applied requirements (Figure 1):

- Regulations, rules and standards of nuclear and radiation safety in force in Ukraine (NP 1999; NP, 2000; NP, 2003a; NP, 2003b; NP, 2005; NP, 2008a; NP, 2008, IEC, 2006b; NAPB, 2000; PNAE, 1987).
- Safety standards of the International Atomic Energy Agency (IAEA, 2000; IAEA, 2002a; IAEA, 2011a; IAEA, 2012).
- Standards of the International Electrotechnical Commission, applicable to Instrumentation and control systems, important to NPPs safety (IEC, 1996; IEC, 1998; IEC, 2005a; IEC, 2007a; IEC, 2007b; IEC, 2011).
- International industrial standards (IEC, 2001a-IEC,2001g; IEC 2002a- IEC 2002c; IEC 2004; IEC 2005b; IEC 2006a; International Special Committee on Radio Interference- CISPR 2006 and ISO 2000).
- State standards of Ukraine (DSTU IEC, DSTU CISPR, DSTU ISO), identical with relevant international standards.

Conformance to requirements of these documents, reflecting long-term national and foreign experience in standardization, assurance and assessment of safety of systems and their components applied in NPP, was supervised by State Nuclear Regulatory Authority of Ukraine and considered as one of the main conditions for issuing a permit for manufacturing and implementation of safety important I&C systems.

It should be noted that regulations NP, 2000 и NP, 2008,a in force are currently revised for harmonization with requirements of new international standards (IAEA, 2011,a; IAEA 2012, etc.), and also with regard to results of practical application and suggestions of interested organizations and NPPs for their improvement. Supposed changes were considered as far as possible in this chapter (and further chapters of the book).

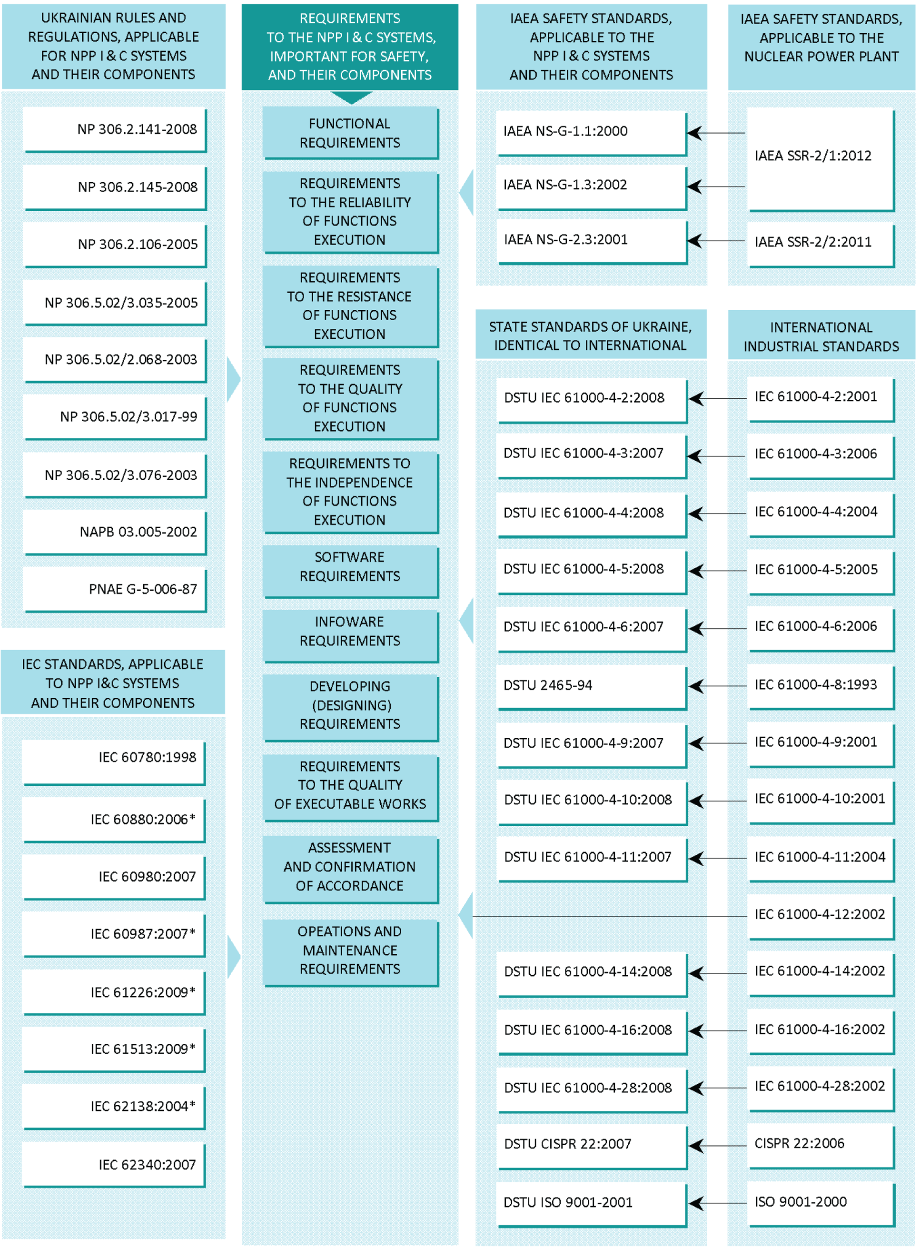
FUNCTIONAL PROPERTIES

According to IEC, 2011 functions, systems and equipment of the NPP may be considered from two points of view – functional and system.

Functional Point of View

This point of view illustrated in Figure 2 considers only the functions to be performed. Instrumentation and control (I&C) function is determined as a specific *objective* that should be reached without mentioning physical means for its achievement. This concept is applied by production engineers to formulate a general task for the whole set of NPP

Figure 1. Rules, regulations, and standards governing the properties of I&C systems and their components



UKRAINIAN RULES AND REGULATIONS, APPLICABLE FOR NPP I & C SYSTEMS AND THEIR COMPONENTS

- NP 306.2.141-2008
- NP 306.2.145-2008
- NP 306.2.106-2005
- NP 306.5.02/3.035-2005
- NP 306.5.02/2.068-2003
- NP 306.5.02/3.017-99
- NP 306.5.02/3.076-2003
- NAPB 03.005-2002
- PNAE G-5-006-87

IEC STANDARDS, APPLICABLE TO NPP I&C SYSTEMS AND THEIR COMPONENTS

- IEC 60780:1998
- IEC 60880:2006*
- IEC 60980:2007
- IEC 60987:2007*
- IEC 61226:2009*
- IEC 61513:2009*
- IEC 62138:2004*
- IEC 62340:2007

REQUIREMENTS TO THE NPP I & C SYSTEMS, IMPORTANT FOR SAFETY, AND THEIR COMPONENTS

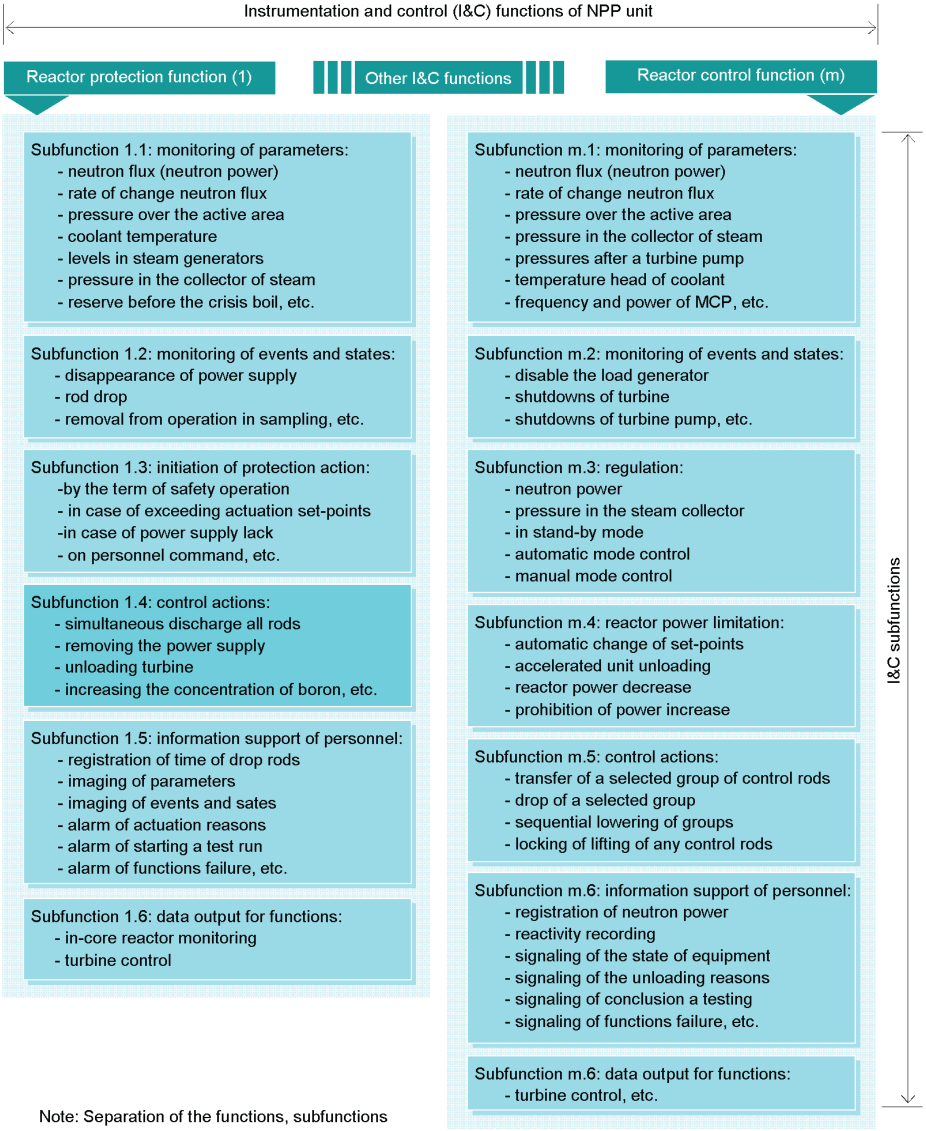
- FUNCTIONAL REQUIREMENTS
- REQUIREMENTS TO THE RELIABILITY OF FUNCTIONS EXECUTION
- REQUIREMENTS TO THE RESISTANCE OF FUNCTIONS EXECUTION
- REQUIREMENTS TO THE QUALITY OF FUNCTIONS EXECUTION
- REQUIREMENTS TO THE INDEPENDENCE OF FUNCTIONS EXECUTION
- SOFTWARE REQUIREMENTS
- INFOWARE REQUIREMENTS
- DEVELOPING (DESIGNING) REQUIREMENTS
- REQUIREMENTS TO THE QUALITY OF EXECUTABLE WORKS
- ASSESSMENT AND CONFIRMATION OF ACCORDANCE
- OPEATIONS AND MAINTENANCE REQUIREMENTS

IAEA SAFETY STANDARDS, APPLICABLE TO THE NPP I & C SYSTEMS AND THEIR COMPONENTS	IAEA SAFETY STANDARDS, APPLICABLE TO THE NUCLEAR POWER PLANT
IAEA NS-G-1.1:2000	IAEA SSR-2/1:2012
IAEA NS-G-1.3:2002	
IAEA NS-G-2.3:2001	IAEA SSR-2/2:2011

STATE STANDARDS OF UKRAINE, IDENTICAL TO INTERNATIONAL	INTERNATIONAL INDUSTRIAL STANDARDS
DSTU IEC 61000-4-2:2008	IEC 61000-4-2:2001
DSTU IEC 61000-4-3:2007	IEC 61000-4-3:2006
DSTU IEC 61000-4-4:2008	IEC 61000-4-4:2004
DSTU IEC 61000-4-5:2008	IEC 61000-4-5:2005
DSTU IEC 61000-4-6:2007	IEC 61000-4-6:2006
DSTU 2465-94	IEC 61000-4-8:1993
DSTU IEC 61000-4-9:2007	IEC 61000-4-9:2001
DSTU IEC 61000-4-10:2008	IEC 61000-4-10:2001
DSTU IEC 61000-4-11:2007	IEC 61000-4-11:2004
	IEC 61000-4-12:2002
DSTU IEC 61000-4-14:2008	IEC 61000-4-14:2002
DSTU IEC 61000-4-16:2008	IEC 61000-4-16:2002
DSTU IEC 61000-4-28:2008	IEC 61000-4-28:2002
DSTU CISPR 22:2007	CISPR 22:2006
DSTU ISO 9001-2001	ISO 9001-2000

Note: * – There are State standard of Ukraine, identical to this standard

Figure 2. I&C functions: examples of a functional point of view



Instrumentation and control (I&C) functions of NPP unit
Reactor protection function (1)
Other I&C functions
Reactor control function (m)
I&C subfunctions

Subfunction 1.1: monitoring of parameters:
- neutron flux (neutron power)
- rate of change neutron flux
- pressure over the active area
- coolant temperature
- levels in steam generators
- pressure in the collector of steam
- reserve before the crisis boil, etc.

Subfunction 1.2: monitoring of events and states:
- disappearance of power supply
- rod drop
- removal from operation in sampling, etc.

Subfunction 1.3: initiation of protection action:
-by the term of safety operation
- in case of exceeding actuation set-points
-in case of power supply lack
- on personnel command, etc.

Subfunction 1.4: control actions:
- simultaneous discharge all rods
- removing the power supply
- unloading turbine
- increasing the concentration of boron, etc.

Subfunction 1.5: information support of personnel:
- registration of time of drop rods
- imaging of parameters
- imaging of events and sates
- alarm of actuation reasons
- alarm of starting a test run
- alarm of functions failure, etc.

Subfunction 1.6: data output for functions:
- in-core reactor monitoring
- turbine control

Subfunction m.1: monitoring of parameters:
- neutron flux (neutron power)
- rate of change neutron flux
- pressure over the active area
- pressure in the collector of steam
- pressures after a turbine pump
- temperature head of coolant
- frequency and power of MCP, etc.

Subfunction m.2: monitoring of events and states:
- disable the load generator
- shutdowns of turbine
- shutdowns of turbine pump, etc.

Subfunction m.3: regulation:
- neutron power
- pressure in the steam collector
- in stand-by mode
- automatic mode control
- manual mode control

Subfunction m.4: reactor power limitation:
- automatic change of set-points
- accelerated unit unloading
- reactor power decrease
- prohibition of power increase

Subfunction m.5: control actions:
- transfer of a selected group of control rods
- drop of a selected group
- sequential lowering of groups
- locking of lifting of any control rods

Subfunction m.6: information support of personnel:
- registration of neutron power
- reactivity recording
- signaling of the state of equipment
- signaling of the unloading reasons
- signaling of conclusion a testing
- signaling of functions failure, etc.

Subfunction m.6: data output for functions:
- turbine control, etc.

Note: Separation of the functions, subfunctions and their numbers are conventional

structures, systems and equipment required and sufficient for realization a proper instrumentation and control function (achievement of the stated objective). According to the terminology used in IEC, 2011, this set can be called "systems and equipment associated with function." A functional point of view is typical for standards IAEA, 2002,a; IAEA, 2012; IEC, 2009, etc.

Monitoring of nuclear fuel fission and reactivity relates to category B functions and provides:

Safety functions are performed to prevent design basis accidents and control accidents (limitation of their effect, prevention of accidents with severe core damages). To safety I&C functions include emergency reactor protection, heat removal from the core and cooling pool, prevention or limitation of radioactive releases release beyond established boundaries.

Reactor protection function provides core transfer of the core to safety (subcritical) state and keeps the shutdown reactor in subcritical state.

Heat removal function provides:

- Coolant inventory monitoring and maintain at the design specific level.
- Emergency core cooling during initiating events, in allowed y the design, in emergencies and/or during design basis accidents and long-term maintenance of core temperature parameters in the design specific limits.
- Residual removal and transfer to the ultimate heat sink from intermediate heat removal used for emergency cooling.
- Retention of the specified (or permissible) level of each parameter controlled during accident management and post-accident mode (for example pressure in the primary circuit, discharge pressure in emergency cooling pumps and emergency feedwater pumps, water temperature in the cooling pool, etc.)

Function of prevention or limitation of radioactive releases in accidents, provide:

- Isolation of the containment and ways of possible distribution of radioactive releases in of postulated initiating events.
- Detection of explosive gas concentrations in rooms under the containment.
- Pressure and temperature reduction and environment decontamination during design basis accidents.

Safety functions are related to category A functions according to IEC 2009.

Normal operation functions are intended to ensure safety of the unit in operation modes (start-up, power generation, scheduled shutdown and cooling), automation of determined activities in standby modes and detection and prevention of threats to personnel or equipment. Examples of normal operation I&C functions: core monitoring; monitoring of nuclear fuel fission and reactivity; control of technological processes of the primary circuit; monitoring of radiation situation; detection and limitation of effects of hazardous events; refueling control.

Core monitoring relates to category B functions and provides:

- Information on neutron physical, thermohydraulic and other parameters, defining core state and operating processes in it.
- Calculation of distribution of neutron flux and power density field in the core.
- Display of obtained information in the form convenient for perception and analysis by operational personnel.
- Testing of conformance between design and real core characteristics.
- Warning of personnel and delivery of signals, initiating performance of reactivity control functions, if deviation of core characteristics from design values exceeds permissible ones.
- Archiving, storage during the specified time period, display and / or registration of core parameter values in case of normal operational occurrences, emergencies, during and after design-basis accidents conformance of heat power of the reactor and turbine during power output in the grid, routine startup and power unit shutdown, and also during rapid load changes, caused by sudden connection or disconnection of high-power loads, energy sources, transmission lines, etc.
- Reactor unloading (heat power reduction) if any conditions of normal operation are

violated and power reduction on the permissible safety level.

- Reactor power reduction if any case of the controlled parameters exceeds the specified limits and also in other cases covered by design or by the operator's initiative.
- Prohibition of reactor power increase.
- Continuous monitoring of reactivity control tools (control rod position; concentration of dissolved neutron absorber in the primary coolant and in the cooling pool; pressure, level and concentration in the emergency tanks with soluble neutron absorber), warning of personnel about violations, display of monitoring results.

Control of technological processes of the primary t circuit of the nuclear installation relates to category A or B functions and provides:

- Compensation of coolant volume change in the primary circuit (automatic level control in the volume compensator).
- Protection against inadmissible increase of pressure in the first circuit.
- On-line monitoring of coolant level in the reactor vessel, activity and content of neutron absorbers in the coolant of the primary circuit.
- Warning of personnel when limits, specified for emergency reserve of soluble absorber in any storage, are achieved.
- Coolant leak detection in the primary circuit, detection of its location and assessment of coolant flow in leak.

Monitoring of radiation situation relates to functions of category C and provides:

- Continuous measurement of parameters, defining radiation situation in the rooms and on NPP territory, in sanitary protection zone and control area.
- Archiving, storage during the specified period of time, display and/or registration of information on radiation situation in each control point, determined by the design, during normal operation, in emergencies, during and after accidents, including beyond design mode.
- Detection of radioactive releases and discharges into the environment, that exceed the limits allowed by the design and warning of operational personnel (preventive and emergency alarm) about excess of allowed parameter limits, defining radiation situation at control points.

Detection and limitation of effects of hazardous events, considered in the design (fire, earthquake, radioactive release, violation of conditions for safety storage of nuclear fuel and radioactive waste, etc.) relate to category A functions. For example, detection and limitation of fire effects provides:

- Automatic detection of fire source by smoke, temperature increase and other signs.
- Signal reception from manual fire detectors.
- Visible and audible warning of fire.
- Formation and issue of a sequence of instructions, initiating disconnection of room ventilation systems, in which fire sources were detected, shutdown of smoke control system and closing of fire retardant valves.
- Formation and issue of instructions, initiating launch of automatic fire fighting system and / or reception of instructions from

manual fire detectors and issue of proper control actions for warning devices and actuating elements of ventilation systems and firefighting systems.

Monitoring and control of refueling relate to category A functions and provides:

- Automatic control of refueling device according to the program, schedule and cartogram of refueling;
- Automatic measuring of neutron flux density and a concentration of fluid neutron absorber solution during refueling.
- Speed limit of transfer of fuel assembles on the levels regulated in the design of refueling machine.
- Protection against damage, deformation, destruction or fall of fuel rod arrays, and also of stress application, exceeding maximal permissible, during their removing or mounting.
- Mechanical locking of refueling device at the limits of permissible transfers of fuel assemblies, and also in case of detection of the beyond design state, failures or damages of refueling device, power loss and initiating events considered by the design.
- Immediate display of information of position, transfer and orientation of fuel assemblies and pinchers.
- Monitoring using closed circuit television system.

Individual functions can be arbitrary divided into parts (subfunctions), for example, for reactor protection function (see Figure 2): monitoring of technological parameters; monitoring of events and states of equipment; initiation of protection action; realization of control actions; information support of personnel; data output required for execution of other functions.

System Point of View

This point of view considers the systems as an organized set of equipment that implements multiple functions/subfunctions. This point of view is typical for designers of overall I&C systems, based on the analysis of functions specified by processing engineers, selection of individual I&C systems required for their implementation and identification of functions, to be performed by each of them (Figure 3). Upon that an individual I&C system can participate in performance of one or several different functions, including those related to different categories.

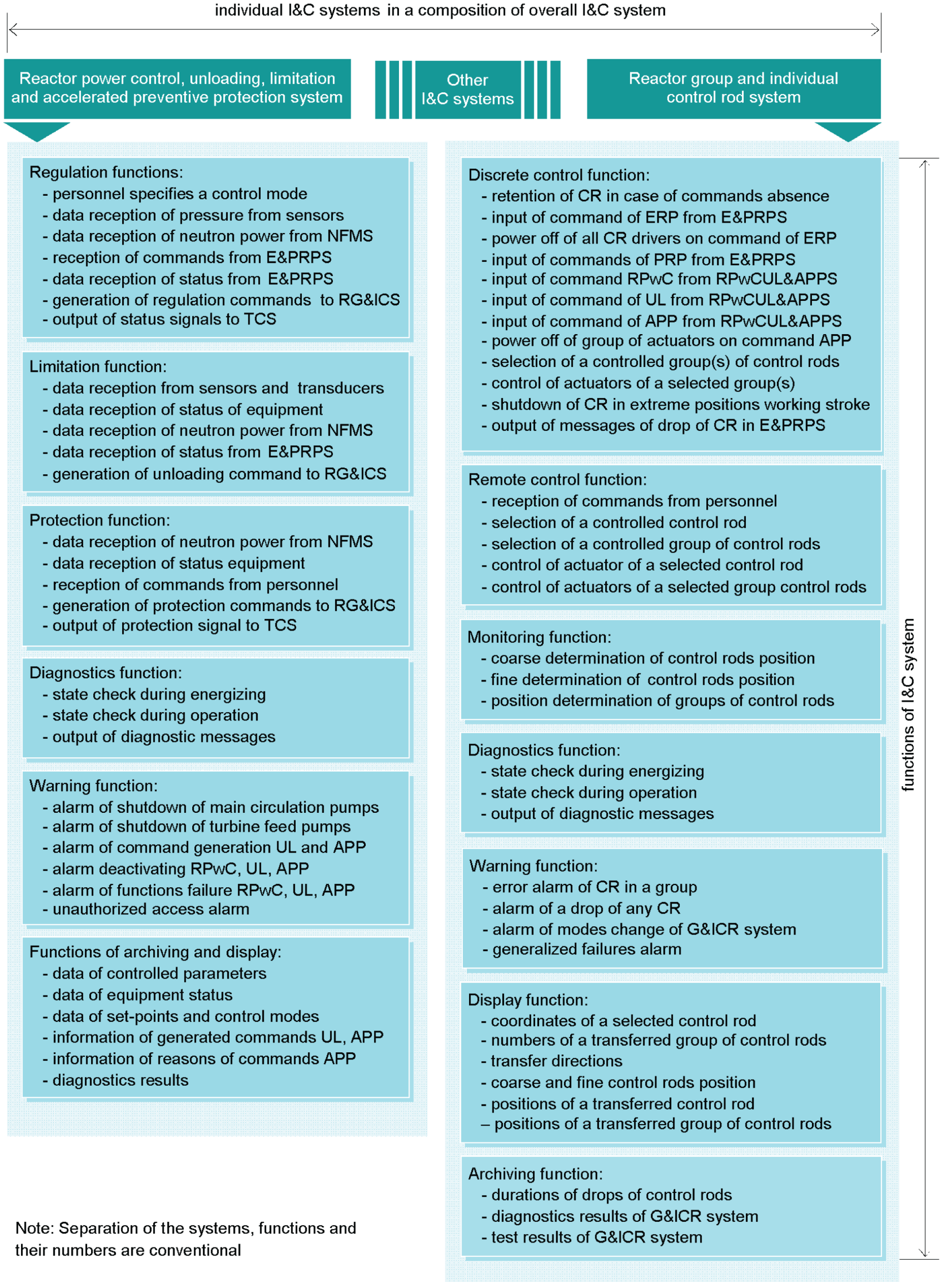
Category of any function of I&C system is determined according to the highest from the categories of relevant functions, in which performance it participates (one and the same function in different I&C systems can relate to different categories).

Safety I&C systems together with technological systems and equipment perform functions required for safety assurance during power unit operation in all operation modes, violations of normal and safety operation and post-accident mode, caused by any design-basis accident.

According to IAEA 2002, a safety I&C systems are divided into:

- Protection systems control operation of technological systems and equipment of power unit and automatically initiate protective actions required to prevent exceeding of design limits, define dangerous or potentially dangerous power unit state, or limit effects of design-basis accidents.
- Safety actuation systems control operation of technological systems and equipment,

Figure 3. Functions of I&C systems: examples of a system point of view



individual I&C systems in a composition of overall I&C system

Reactor power control, unloading, limitation and accelerated preventive protection system

Other I&C systems

Reactor group and individual control rod system

Regulation functions:
- personnel specifies a control mode
- data reception of pressure from sensors
- data reception of neutron power from NFMS
- reception of commands from E&PRPS
- data reception of status from E&PRPS
- generation of regulation commands to RG&ICS
- output of status signals to TCS

Limitation function:
- data reception from sensors and transducers
- data reception of status of equipment
- data reception of neutron power from NFMS
- data reception of status from E&PRPS
- generation of unloading command to RG&ICS

Protection function:
- data reception of neutron power from NFMS
- data reception of status equipment
- reception of commands from personnel
- generation of protection commands to RG&ICS
- output of protection signal to TCS

Diagnostics function:
- state check during energizing
- state check during operation
- output of diagnostic messages

Warning function:
- alarm of shutdown of main circulation pumps
- alarm of shutdown of turbine feed pumps
- alarm of command generation UL and APP
- alarm deactivating RPwC, UL, APP
- alarm of functions failure RPwC, UL, APP
- unauthorized access alarm

Functions of archiving and display:
- data of controlled parameters
- data of equipment status
- data of set-points and control modes
- information of generated commands UL, APP
- information of reasons of commands APP
- diagnostics results

Discrete control function:
- retention of CR in case of commands absence
- input of command of ERP from E&PRPS
- power off of all CR drivers on command of ERP
- input of commands of PRP from E&PRPS
- input of command RPwC from RPwCUL&APPS
- input of command of UL from RPwCUL&APPS
- input of command of APP from RPwCUL&APPS
- power off of group of actuators on command APP
- selection of a controlled group(s) of control rods
- control of actuators of a selected group(s)
- shutdown of CR in extreme positions working stroke
- output of messages of drop of CR in E&PRPS

Remote control function:
- reception of commands from personnel
- selection of a controlled control rod
- selection of a controlled group of control rods
- control of actuator of a selected control rod
- control of actuators of a selected group control rods

Monitoring function:
- coarse determination of control rods position
- fine determination of control rods position
- position determination of groups of control rods

Diagnostics function:
- state check during energizing
- state check during operation
- output of diagnostic messages

Warning function:
- error alarm of CR in a group
- alarm of a drop of any CR
- alarm of modes change of G&ICR system
- generalized failures alarm

Display function:
- coordinates of a selected control rod
- numbers of a transferred group of control rods
- transfer directions
- coarse and fine control rods position
- positions of a transferred control rod
– positions of a transferred group of control rods

Archiving function:
- durations of drops of control rods
- diagnostics results of G&ICR system
- test results of G&ICR system

functions of I&C system

Note: Separation of the systems, functions and their numbers are conventional directly performing initiated protective actions and monitoring the state and operation of this equipment.

- Safety systems support features control and / or control operation of technological systems and equipment, creating required operation conditions of protection– and actuation systems (for example, emergency power supply, safety equipment cooling, provision of working environment, etc.)

Protection I&C *systems* initiate protective actions in any postulated initiating event, which can lead to emergency: violations of any of safety operation conditions; dangerous external effects; failure of the protection system; exceeding of any of its controlled parameters (including design ones) or a specified combination of parameters beyond the limit, determined by the relevant set-point. Operational personnel in the main control room or emergency control room may at any time issue a command, by which the protection system initiates performance of protective actions.

The Design and Technical Specification for Safe Operation for each protection I&C system the following is specified: conditions for initiation of protective actions; a list of command receivers (safety actuation I&C systems and / or actuating elements of technological safety systems); required lags of issue and / or withdrawal of commands (if necessary); compliance of logic conditions of each discrete output signal (command) with values of physical quantity, applied for representation of these states. This compliance is selected on the basis of qualitative evaluations of probability of inaccurate interpretation of an output signal by a receiver (caused by failures of components of a protection system, communication line, etc.) and severity of effects, to which such a fault can lead. For example, in the reactor protection system issue of commands, initiating emergency power unit shutdown, corresponds to a high resistance or output circuit break of this signal source, command withdrawal to – low resistance (or closing) of output circuit.

Set-points of technological parameters of protection I&C system can be constant or variable (depending on other parameters and / or conditions). In the design of protection I&C system provides means that allow retrieving actual values of set-points during operation and, if necessary, changing them within the limits, allowed by the design. Change of set-points is performed by personnel of NPP, using specifically provided hardware and software, contained in the protection system, all changes are controlled and archived.

During unit operation or in standby modes the protection I&C system performs described in Chapter 1 main and auxiliary functions of monitoring, archiving, warning (preventive alarm), display, diagnostic and archiving:

- Monitors parameters, events and states, defining specified conditions of initiating protective actions.
- Monitors technical state of its components and adjacent equipment.
- Diagnoses operability failure that may lead to a situation, when a system will be unavailable to perform safety functions, and warns operational personnel of detected disturbances.
- Archives and displays values of controlled parameters and diagnostic messages of technical states of its components and adjacent equipment.

In case of operational events the protection I&C system, having initiated any of the specified conditions of protective measures, performs protection functions, warning (emergency alarm), display and archiving:

- Warns operational personnel of system actuation and displays information on the condition (“cause of system actuation.”)

- Generates and issues command sequence required for a complete performance of design specific protective actions (even in case when the cause, provoked actuation of the protection I&C system, disappeared) into safety actuation I&C systems and / or for actuating elements.
- Displays information required for operational personnel to monitor system operation, check operation accuracy, initiate, if necessary, allowed actions intended for safety assurance, and check their results.
- Archives: data on cause of system actuation; values of controlled parameters; information, describing technical state of its components and adjacent equipment; data of commands and directions obtained from the operational personnel and adjacent systems.

After actuation of protective actions, a possibility to execute power unit shutdown of the whole protection I&C system or its individual commands within a project specific time period (for example, for reactor protection system – not less than 10 min according to NP, 2008,a) is automatically blocked. This does not prevent performance of other functions, which can be required for safety assurance (except those, which are not compatible with performed protective actions), in particular, the operational personnel in the main (or emergency) control room may duplicate specific commands, initiate actuation of protective actions by other protection systems, etc.

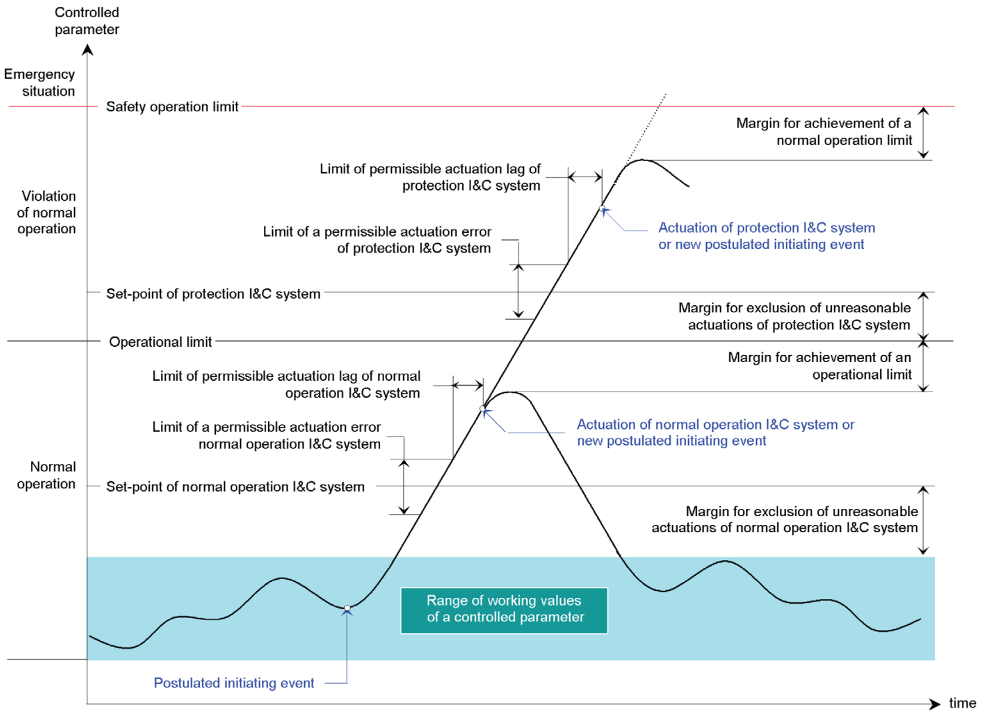
Issued commands are retained at the output of the protection I&C system until a complete performance of initiated protective actions, even after the reason caused them was eliminated. Returning the protection I&C system in the initial state and withdrawal of all its issued commands are performed by the actions of operational personnel specified in the design.

During determination of set-points probable (permissible) errors and lags of actuation of the protection I&C system, and also expected transient processes during performance of protective actions are considered, so that in any postulated initiating events controlled technological parameters did not exceed the design specific limits of unit safety operation (see Figure 4). Limits of safety operation specified on the basis of safety criteria and determine limiting values of controlled technological parameters; if they are exceeded, effects unacceptable for power unit safety can be expected (IAEA, 2002,a) (according to NP, 2008,a exceeding the limit of safety operation may lead to an emergency). To exclude unreasonable actuation of the protection system provides required margins between the specified set-points and operational limits of relevant technological parameters, which were specified in the design for a normal operation of the unit.

Operability failure of components of the protection I&C system are detected automatically. Operational personnel are immediately warned about failures, which may lead to a situation, when a system will be unavailable to perform required safety functions with the specified reliability and quality. Possibility of unit operation in case of components' failure of the safety protection system, acceptable operational limits and restrictions and also time, during which operation is allowed in such conditions, are agreed with Ukrainian Regulatory Authority and specified in Technical Specifications of Safe Operation and in documents, substantiating safety.

Safety actuation I&C systems perform functions of display, warning (preventive alarm), archiving, discrete control and / or regulation (see Chapter 1). During power unit operation in operating modes the safety actuation system: controls technical state and diagnoses operability failure of its components and adjacent equipment; warns operational personnel about failures, which may lead to a situation, when a system will be unavailable to perform specified functions; archives and displays diagnostic results.

Figure 4. Design limits and selection of set-points of I&C systems


Controlled parameter
Emergency situation
Safety operation limit
Margin for achievement of a normal operation limit
Limit of permissible actuation lag of protection I&C system
Violation of normal operation
Limit of a permissible actuation error of protection I&C system
Actuation of protection I&C system or new postulated initiating event
Set-point of protection I&C system
Margin for exclusion of unreasonable actuations of protection I&C system
Operational limit
Margin for achievement of an operational limit
Limit of permissible actuation lag of normal operation I&C system
Limit of a permissible actuation error normal operation I&C system
Actuation of normal operation I&C system or new postulated initiating event
Normal operation
Set-point of normal operation I&C system
Margin for exclusion of unreasonable actuations of normal operation I&C system
Range of working values of a controlled parameter
Postulated initiating event
time

In case of operational events the safety actuation I&C system:

- By commands from the safety protection I&C system forms and issues control signals to actuating elements of technological systems and equipment (gate valves, pumps, electric motors, control valves, control rod drives, etc.) required for performance of protective actions initiated by these commands.
- Prohibits execution of commands that can be issued by other protection I&C systems, normal operation I&C systems and / or operational personnel in case they are not compatible with executed protective actions.
- Displays information required for operational personnel to control executed actions and if necessary perform remote control of technological equipment.
- Archives data of commands, obtained from the safety protection I&C system, normal operation I&C systems and operational personnel, results of automatic diagnostic and detected operability failures of own components and adjacent equipment.
- Forms and issues messages to other I&C systems about condition of operation of own components and adjacent equipment.

For each safety actuation I&C system the following is defined in the design: a list of sources of commands (safety actuation I&C systems, normal operation I&C systems, equipment of main control room and / or emergency control room); a list of command receivers (actuating elements of technological systems and equipment); algorithms for formation of control signals required delays of output and / or withdrawal of control signals (if necessary); compliance of logic conditions of each discrete output signal with values of physical parameters, applied for representation of these states. Selection of such compliance is performed on the basis of signal receiver properties. For example, for execution of protective action initiated by command of the reactor protection I&C system (dropping of all control rods into core that causes emergency shutdown of reactor), outputs of reactor group and individual control rod system are transferred by this command and retained in active logical condition that is complied with a lack of current in circuits, connecting these outputs with all control rod drives. In the absence of a command of emergency protection, logical state of outputs provides direct current in these output circuits.

Safety systems support features that perform information functions of monitoring, warning, display, archiving and control functions of regulation, locking, discrete and remote control described in Chapter 1. As an example the automatic control system of diesel-generator used at Ukrainian NPP (see Belohin et al, 2010) can be given.

During power unit operation or in standby modes, automatic control system of diesel-generator:

- Supports Diesel: Generator in constant readiness for start-up and fast load acceptance.
- Provides periodic checks (testing) of each diesel-generator at zero load and with a load on the a unit electrical network (including synchronization of shaft speed with network frequency and change of generator reactive capability).
- Continuously controls technical state and diagnoses operability failure of its own components, adjacent peripheral equipment and connecting lines, archives diagnostic results and transfers them to the main control room for display and warning of personnel about failures, which can lead to the system unavailability for execution of specified functions.

In case of operational events, the automatic control system of diesel-generator forms and issues control signals, providing:

- Start-up of a diesel-generator by a command obtained from the safety protection I&C system and operational personnel, including required operations and further automatic mutual synchronization of rotation speed of two diesel-generators, operating into a total load.
- Automatic support of required parameters of a diesel-generator during a long period of time, operating at a full capacity, including refill of the service tanks of fuel, oil, coolant, etc.
- Execution of manual (remote) control commands: changing of active and reactive generator power, connection and disconnection of auxiliary equipment.
- Automatic emergency shutdown of a diesel-generator (with locking of the next launch) in case of actuation of uninterruptable protective means of technological equipment (other protective means are disconnected in order that functions of safety system support features had a priority over equipment protection functions).
- Automatic shutdown of a diesel-generator by a command obtained from personnel, including operations, which provide availability of a diesel-electric unit for the next start-up.
- Warning of personnel (indicating alarm) about execution of start operation, operation at a capacity and shutdown.
- Continuous monitoring, archiving, display and register of parameters of a diesel-generator, adjacent equipment, events and conditions during operation of a diesel generator.

Normal operation I&C systems together with technological systems and equipment and operational personnel perform functions required for safety assurance during power unit operation in all operating and standby modes, including in case of detection of threats to personnel, population, environment or equipment (see 3.1.1).

As examples of normal operation I&C systems ones applied at NPP units in Ukraine: in-core reactor monitoring systems (Gorelik, 2005); computer information systems and safety parameters display systems (Anikanov, 2003 and Chapter 11 this book), reactor power control, unloading, limitation and accelerated preventive protection systems (Bachmatch, 2005), fire-alarm systems (Bachmatch, 2008).

Normal operation I&C systems together with technological equipment and operational personnel perform functions intended for monitoring and control of technological processes and prevention of operational events:

- Retains controlled parameters within working values in conditions of external and internal influences, possible for specific operating or standby mode (see Figure 4).
- Display information required for operational personnel that controls process flow, operation of technological equipment of normal operation system, condition of physical barriers on the path of ionizing radiation and radioactive substances.
- Automate operational personnel actions, for example, during increase or reduction of power unit capacity, scheduled shutdown and cooling, refueling, etc.
- Monitoring technical state of own components and adjacent equipment, diagnose, archive and display failures, which can lead to to the system unavailability for execution of specified safety important functions with a specified reliability and quality, warn personnel about such failures.
- Identify occurrence of conditions, which can lead to operational events (exceeding operational limits, specified by the design for controlled parameters) and require preventive action to prevent this event.
- Automatically initiate actions of other I&C systems required for prevention of operational events and / or control technological equipment, performing these actions.
- Warn operational personnel about possible operational events (preventive alarm in the main control room) and automate its actions intended for prevention of such violations.

Conditions, under which normal operation I&C systems initiate preventive actions, can be the following: sudden disconnection of unit technological equipment required for operation at full power; generation shedding; supply frequency reduction of main circulation pumps; design-basis earthquake; detection of ignition signs; transition of a value of any of controlled measured or design parameters over the limit specified by a set-point; reception of a command from an operational personnel from the main control room. Preventive actions, required for prevention of operational events, are reactor power reduction; connection of reserve technological equipment; mechanical braking of device mechanisms of nuclear fuel overload; connection of an automatic fire fighting system, etc. Control of technological equipment, performing preventive actions, can provide, for example, issuing control influences to control rod drives.

During specification of set-points possible (permissible) errors and actuation lags of the normal operation I&C system and also expected transient processes during execution of preventive actions are considered, so that controlled technological parameters in any point of time do not exceed specified in the design operational limits (IAEA, 2002,a) determines operational limits as restrictions for technological variable and other important parameters, at which operation of NPP is allowed. According to NP 2008,a deviation from specified in the design operational limits that did not cause emergency is considered as an operational event).

To except execution of unnecessary preventive actions, a margin between upper limit of working values of each of controlled parameters and a value of a set-point, specified for it in the normal operation of the I&C system, is provided.

Failures of components, which can cause unavailability of the normal operation I&C system for performance of required safety important functions with a specified reliability and quality, are automatically detected and displayed in such a form that simplifies taking measures for operability recovery by personnel.

Possibility to continue power unit operation in case of components' failures of safety important normal operation I&C systems, allowed design limits and restrictions and time, during which operation in such conditions is allowed, is specified in Technical Specification on Safe Operation.

Post-accident monitoring systems provide informational support of personnel and safety experts during control of accidents, elimination of their effects and return of reactor facility into controlled state, and also during the process of further analysis of occurrence reasons and behavior of design and beyond design basis (including severe ones) accidents.

For this purpose post-accident monitoring systems perform monitoring functions, archiving, display and register of data of occurrence of initiating events, emergencies and accidents, actions of a protection system and operational personnel, intended for safety assurance, and also about controlled thermo-hydraulic, neutron physical and other parameters, defining a state of power unit and protection systems, integrity of physical barriers (fuel matrix, fuel claddings, boundaries of the primary coolant system and containment), radiation environment in rooms and on the NPP territory, in sanitary protection zone and control area.

Information obtained from I&C system of post-accident monitoring is supposed to be used for:

- Identification of a postulated initiating event that was a cause of failure of a specified operating limit(s); recreation of a sequence of further events, including protective actions of safety systems and / or operational personnel; to be convinced that during the execution of these actions limits of safety operation were not exceeded and physical barriers on a way of spread of radioactive substances and ionizing radiation were undamaged.
- Identification of the cause, that provoked an emergency situation, and recreation of the sequence of further events, including actions of operational personnel to return unit in a normal operation; assessment of possible effects of exceeding normal operation limits; to be convinced that release of radioactive substances and ionizing radiation did not exceed the limits specified by the design.
- Identification of a cause and recreation of the sequence of events in development of the emergency into an accident; analysis of release of radioactive substances and / or ionizing radiation over specified limits; execution of required actions for accident control; detection of necessity to take off-site emergency actions.
- Assessment of damages to structures, systems and components, including physical barriers, caused by design basis or beyond design basis accident, and use of these data during mitigation of its effects.

The design of I&C system of post-accident monitoring regulates lists of considered initiating events and monitored parameters and determines their qualitative properties and ranges of variation, possible in conditions of emergencies, design basis and beyond design basis accidents, also including those values of monitored parameters at which integrity and efficiency of physical barriers can be disturbed.

Means for display and record of information that included in the post-accident monitoring system are placed in the main – and emergency control room and in rooms of internal (on-site) and external (in supervised area) crisis centers. Information is saved in an archive of the post-accident monitoring I&C system and should be kept undamaged in case of accidents, including severe ones. Measures for protection of archival data from unintended or intentional change during the specified period of time are provided.

Combinations of Functions in I&C Systems

One I&C system can combine different functions to achievement and maintain of safety which can be related to different categories according to IEC, 2009. Failure to perform a function in such a system does not influence the possibility to perform other functions of the same and higher category.

In normal operation I&C systems, closely functions are usually combined (in various combinations), for example: monitoring, display and registration; limitation, locking and warning; discrete (automatic) and remote (manual) control. In the last case in order not to create obstacles for automatic control in case of failures in manual control circuits (and vice versa), the number of elements, taking part in performance of one or another function, is minimized. The difference between categories of performed functions is often occurred due to combination of safety functions in one system (for example, emergency reactor protection) and normal operation function (preventative reactor protection), but safety functions have a *priority* over normal operation functions, and such a combination will not lead to reliability reduction and / or degradation of other system properties, defining performance of safety functions.

The functions, combined in one system, can be distributed among several software-hardware complexes contained in it (SHC), though for modern I&C systems combination of functions in one SHC that performs not only all the main, but also additional (auxiliary and service) functions is more typical (main system function are determined by its purpose, auxiliary functions provide continuous automatic monitoring of system technical state, display, archiving and warning of personnel about operability failures and attempts of unauthorized access, service functions– automate actions of personnel during reconfiguration, periodic tests, etc.). In this case required measures are taken in order that auxiliary functions (which can be performed simultaneously with main ones) and / or failures of associated equipment of SHC will not lead to degradation of properties of the I&C system, defining performance of main functions. Resistance of these properties to component failures of SHC, intended for implementation of service functions, performance of which is usually not intersected during performance of main functions, is also provided.

Combination of functions of protection system and safety actuation system in one safety I&C system can be justified if this does not have negative influence on safety. However, such a combination is inadmissible, when protective actions initiated by the protection I&C system, should be performed by divers safety actuation systems, which reserve each other (for example, disconnection of hold current of each of control rod drives is duplicated by damping of force electrical power simultaneously from all drives).

Reconfiguration of the I&C System

In cases, when actions of the I&C system, specified by the design for a specific operating or standby mode of a power unit, can prevent its transfer to another mode, system reconfiguration is provided, for example, intentional prohibition of issuing unnecessary individual commands and their performance in a new mode becomes needless and undesirable (in the international standard IAEA, 2002,a such blocks are called "operational bypasses").

For the safety I&C system, operational bypasses are possible after authorized transfer of SHC into a special mode and only for a limited time period. Data on commands of SHC, whose issue is locked by bypasses, are archived and displayed in the main control room. After locking of one or another command becomes unnecessary, initial system configuration is restored (operational bypass, fixed on a proper output of SHC is disconnected).

Reconfiguration of the safety I&C system or normal operation system can be also required in case of detection of sensor failure, connecting line break, unreliability of received signal or message, etc. if it is impossible to promptly repair a detected failure. In such cases, an operational bypass is executed by a temporary modification of the performed data processing algorithm that eliminates the use of information from a relevant input of SHC.

Reconfiguration of the I&C system can become necessary after execution of some tests during maintenance. Implementation of such changes (mounting of "maintenance bypasses") requires measures to eliminate the possibility of results' falsification during tests with installed bypasses and provide absence of errors after initial system configuration recovery (disconnection of bypasses) at the final stage of maintenance (IAEA, 2002). In particular, procedures of sequential deactivating redundant channels of a safety control system and/or redundant SHC, contained in the system, which eliminate possibility of reconfiguration without receiving a relevant approval and warning of operational personnel, are specified.

Operational personnel in the main control room is immediately warned about unavailability of a system, SHC or channel to perform safety functions, at the same time relevant outputs of the safety I&C system are automatically set in preliminary specified logical state, determined and grounded during safety analysis, in such a way to minimize negative influence of a detected failure on a power unit safety.

RELIABILITY OF I&C FUNCTIONS EXECUTION

Coping with Common Cause Failures

For safety I&C systems and SHC, related to 2(A) safety class, measures for coping with common cause failures - simultaneous failure due to one and the same cause of two or more elements in different redundant parts, which can result in a failure of I&C function of A category are taken (simultaneous failures are considered ones, where a period between them is insufficient to restore operability of the I&C system or SHC after each of such failures). For I&C systems and SHC, related to 3(B) and 3(C) safety classes, requirements for coping with common cause failures are recommended.

As common cause failures the following is considered:

- Appearance of not detected (hidden) errors, which may occur during design, development of hardware and software, production, delivery, assembling, integration, adjustments, maintenance and / or recovery of the I&C system.
- Components interference in the I&C system or SHC through common parts of input, output, power supply, ground circuits

or over the space of rooms, which can reveal itself during operation, connection, disconnection or due to a failure.

- Influence of closely located electrotechnical equipment and / or electrical power cables.
- Deviation from specified ("working") operation conditions, which can be caused by technological equipment failures, abnormal acts of nature (earthquake, lightning stroke), dangerous external or internal events (fire, flood), failures of power supply systems, ventilation systems, etc.

Coping with common cause failures is provided by observance of:

- Principles of single failure, redundancy, diversity, independence, prevention of personnel errors.
- Norms of tolerance (resistance) to influences of external factors.
- Rules of development, quality management, assessment and confirmation of compliance of I&C systems and their hardware and software components with requirements of regulations and standards, active in Ukraine, and also international standards.

Observance of Single Failure Criterion

According to a single failure criterion, I&C systems and SHC, related to 2(A) safety class, should perform all specified functions of A class in any postulated initiating event (PIE), with imposition of failure of one (any) element independent of this PIE. The single failure criterion is also used in relation to a group of I&C systems or SHC, which reserve each other, simultaneously performing safety functions identical for achieved goals. Additionally a possibility of potentially dangerous effects of this PIE and also hidden (undetected by embedded diagnostic facilities) operability failures are taken into account. Single failures of passive elements, properly designed, manufactured and controlled, can be not considered if for a whole period of time after PIE, during which operation of these elements is required, a probability of their failures (considering loads and environmental conditions, including impact of PIE itself) does not exceed agreed minimum allowed value. The criterion is applied independently of a single failure type (nonoperation, false operation) and should consider cases, when a failure of one element causes directly or indirectly dependent on it failures of other elements.

Observance of a single failure criterion means that I&C system (a group of reserving each other I&C systems) or SHC can perform all required category A functions in case of the worst of possible configurations, for example, if during unit operation an initiating event occurred at the time, when individual redundant parts of I&C system or SHC were taken out of operation for inspection during maintenance or recovery (in doing so, it is determined what redundant parts, an order and time period can be simultaneously taken out of operation, a procedure of their termination and further commissioning and also methods of confirmation of operation accuracy after configuration recovery). As agreed by the regulatory body, as an exception, incompliance with the single failure criterion within a limited time period required for inspection is allowed. It is defined on the basis of engineering estimate of reliability so that a possibility of single failure occurrence within this period will not exceed the agreed minimum allowed value specified for a proper function.

Outputs of redundant part of I&C system or SHC that failed or are taken out of operation are automatically determined and held in such sates, which are defined during analysis as the most acceptable from safety point of view.

The single failure criterion is also used in the context of category B functions, at the same time the possibility of hidden operability failures is usually not considered.

Observance of Redundancy Principle

Observance of the determined reliability criteria and single failure criterion for category A functions is provided by redundancy (application of additional means and / or possibilities, redundant with regard to that, are minimally required for function performance). Redundancy supposes the presence of several identical and different components, forming redundant channels of I&C system (or SHC), where each may perform a required function independently of the technical state of other channels. Redundancy of power supply, sources and receivers of data and connecting lines used for transmission of signals and massages between I&C systems, SHC or channels, taking part in performance of category A functions, especially those, access to which during power unit operation is impossible (for example, placed inside the containment), are also provided.

The redundancy approach is selected in such a way that improvement of reliability of performance of required functions was not followed by increase of probability of faulty actions, etc. an acceptable relation between a probability of failure type “nonoperation” and “false operation” was provided. Efficiency of redundancy is provided by:

- Observance of independence principle of power supply of redundant channels, data sources and receivers, connecting lines.
- Continuous automatic monitoring of technical state of redundant channels and diagnostic of operability failures on the level of removable component parts of each channel.
- Operability recovery by operative replacement of a failed removable part of a redundant channel without taking out of operation other channels.

Redundancy of emergency reactor protection function (ERP) is performed in the following way:

- In the structure of ERP system, two independent SHCs, at least, are provided, in each SHC – not less than three independent redundant channels.
- Power supply of each channel is provided through two inputs from different sources of reliable supply.
- Each channel has a complete set of input signals and generates an output signal by any of specified conditions of initiating protective actions.
- In case of disconnection failure of one channel (without taking out of operation the whole SHC) at the output of this channel a trip signal should be automatically determined.
- Each SHC should initiate protective actions by channel trip signals according to a logic condition, selected by results of safety analysis (minimum – “two-out-of-three”).
- Command, initiating protective actions, should transfer from each SHC to an actuating system through, at least, two lines.
- Actuating system should execute specified protective actions by a command obtained from any SHC.
- SHC, taken out of operation, should not in any conditions issue commands, initiating protective actions and prevent actuating system from executing commands obtained from other SHC.

Redundancy of the neutron-flux monitoring system provides that:

- Monitoring of neutron flux density and rate of its change should be executed by two independent sets of equipment (SHC), each of them has, at least, three independent channels.
- In reasoned cases, a neutron flux density monitoring channel and a monitoring channel of rate of its change may have a common measuring part.
- As a data source for ECR an individual set of equipment with three independent monitoring channels is provided.
- For monitoring of neutron flux density during refueling of nuclear fuel, an additional system, having not less than three independent channels, can be provided.

For category B functions redundancy can be reasoned, for example, by expediency of observance of a single failure criterion, specified by requirements for reliability factors, a lack of time for alternative actions in case of a failure of function performance, severity of possible failure effects. In regards to category C functions, redundancy is usually not provided, however in some cases it can be required for achievement of specified reliability (non-failure operation) of performance of these functions.

Observance of the Diversity Principle

According to IAEA, 2011,a diversity is a property related to a group of two or more number of I&C systems and SHC, which simultaneously and independently from each other perform functions identical for achieved safety purposes. The diversity principle provides that these (I&C systems or SHC), forming this group, differ from each other by the operating principle, structure, applied component parts, software and / or other attributes or achieve a target goal in different ways. Differences between elements define, in fact, a diversity type:

- **Design:** Is provided by use of different methods (approaches) for design of hardware and / or software of each element of group.
- **Functional:** Provides difference of algorithms.
- **Signal:** Is achieved by the fact that with different sets of input information each element of a group is able to initiate one and the same protective action.
- **Hardware:** Is provided by the fact that component parts in different elements of group differ by operating principle, manufactured by different technologies and / or obtained from different manufactures.
- **Software:** Provides use of different software modules, programming languages, instrumental tools for software development in each of group elements.
- **Subjective:** Is achieved by elements forming a group and/or their component parts developed by different teams of executers.

The most efficient combination consists of several diversity types, at the same time difference of elements of I&C systems or SHC should be objective, but not to be based only on different manufacturers' (suppliers) names, different titles of one and the same component part, program or other formal attributes.

The diversity is used:

- In order to minimize influence of hidden errors, which can occur at stages of design and packaging of I&C system and / or development and manufacturing of SHC and reveal themselves as a common cause of simultaneous failure of several redundant group elements.

- To overcome difficulties related to obtaining of required confidence that there is no influence from hidden errors and / or to representation of lack of influence.
- Compensates for insufficient approbation of complex I&C systems or SHC by practical operating experience.

According to NP, 2000 observance of the diversity principle is mandatory for a group of I&C systems or SHC, taking part in performance of the emergency reactor protection function. For other category A functions determination of the necessity or suitability of diversity and selection of adequate type(s) of diversity are based on probability analysis of “hidden” errors made during development (design) and manufacturing, which may cause simultaneous failures of several group elements, severity of probable failure effects, degree of approbation, etc. The diversity principle can be not observed if a risk of possible common cause failures, caused by such failures, is admitted as more applicable, comparing to a significant rise in the cost of design, development and operation of diversity I&C systems and SHC, performing the same functions. For a group of independent elements, taking part in performance of category B and C function(s), observance of the diversity principle is not mandatory.

Prevention of Personnel Error

NP 2000 and NP 2008,a consider prevention of personnel error as one of the important factors for safety assurance during intended use I&C systems (during unit control in operating modes and / or accident management), inspections of maintenance and recovery and also in case of reconfiguration.

Operational personnel obtains full, timely and accurate data of specified and current values of controlled technological, neutron-physical and other parameters, state of structures, systems and equipment of unit, initiating events, actions of safety management systems and normal operation systems sufficient for power unit control, timely detection and elimination of normal operation failures, prevention of emergencies, accident control and result estimation.

Redundancy of I&C system components, which take part in functions execution of information display, related to category A (including facilities, placed in the main control room) is provided. To eliminate a possibility of false interpretation of information in case of failure or taking out of operation of one of redundant channels, simultaneous display of values of each parameter, obtained from all channels, is provided, or display only those values, which are considered reliable ones as a result of automatic check or obtained from operable channels (or only one the most reliable value that is defined by automatic processing of information obtained from all channels). There can be no redundancy if nonoperability of an element can be detected and eliminated faster than permissible data loss time, provided that before operability recovery obtained information is displayed together with a clear and unambiguous understanding by personnel of indication of their invalidation.

Data of personnel actions, which can affect safety, are immediately transferred to the main control room (or emergency control room). If control of safety important technological systems and equipment can be performed not only from the main- or emergency control room, but also from other places (for example, with local control panel), visual identification of the place, from where control is performed this moment (the possibility of simultaneous control from different places is precluded) is provided.

Immediate warning of operational personnel about failures of components of I&C systems (SHC, hardware or software), which prevent performance of category A and B function(s), is provided. Relevant emergency (visual and audio) and preventive alarm facilities are placed in the main control room. Prevention of errors, which can lead to a nuclear accident and risk of personnel radiation during overload of nuclear fuel, is provided by the refueling machine control system. Operational personnel and safety experts that control accidents and their effects obtain required data of radiation environment and states of systems, equipment and physical barriers on the way of propagation of ionizing radiation and radioactive substances from the post-accident monitoring system.

Personnel that monitors state of I&C systems, maintains and performs renewal timely and in full scope obtains diagnostic messages, containing data of nonoperable and / or intentionally taken out of operation system components, component parts of SHC and power sources. Diagnostic messages are displayed to facilitate and accelerate the process of making decisions of recovery of operable state of a failed component of the I&C system or a component part of SHC. Display facilities of diagnostic messages are placed in the shift engineer room that monitors state of I&C systems. Also power supply state (presence of operating and standby voltage, switching from the main to emergency power source, etc.) is displayed “by place” and in the main control room.

During development and operation of the I&C systems measures are provided implemented to prevent errors during reconfiguration (adjustment of set-points, rules of control law, conditions of protection initiation, interlocking and alarm, setting and removal of bypasses, taking out and further into operation of individual components for checking during maintenance or after recovery) Allowed reconfigurations can be executed according to rules specified in operational documentation and only by trained personnel that uses specifically intended hardware and software for it. Attempts for making any changes, exceeding permissible limits, are automatically locked and followed by failure alarm. Operational personnel is warned in advance about supposed reconfiguration and informed about its start and completion. In I&C systems, related to 2(A) safety class, a local preventive alarm and warning of operational personnel about an attempt of deactivating channel or SGC, unauthorized and / or not detected from the main control room, is provided, and the possibility of simultaneous deactivation of two redundant channels or two SHCs is precluded.

Component parts during recovery of SHC can usually be replaced without a power dump, in this case any adjustments in component parts of SHC and adjacent products are not required. Specific design solutions prevent a possibility of failure during replacement of component parts and connection of external cables. Apparatus and their removable component parts, related to 2(A) safety class, are labeled in such a way that they can be distinguished from those related to lower safety classes. Labeling of diversity component parts, including those stored in a composition of operating recovery reserves, allows identifying their belonging to a relevant I&C system or SHC.

Protection from Unauthorized Access

For prevention of intentional of unintentional deactivation, reconfiguration, input of interferences, damage or theft, which can create a threat for safety, protection against unauthorized access to the following objects is provided:

- Operating stand-alone devices (hardware).
- Removable component parts and software products, containing in the devices.
- Switching elements for connecting devices to external circuits.
- Elements intended for reconfiguration of the I&C system (SHC).
- Power switches, elements of mode selection and manual control.
- Embedded means for technical diagnostic.
- Means of data input for obtaining access to software, data base and archive.
- Operating recovery reserve and software products, containing in storages.

For protection against unauthorized access, the following is provided: administrative measures (access restriction in premises); physical protection (seals on door locks, cases – safes, etc); software methods (use of passwords, access restriction through external interfaces and service equipment); location of programs and information in write protected memory spaces; alarm, warning access obtaining in the device (for example, open of case doors) and / or attempt of unauthorized modification of programs and information. If access in a device can be required, for example, for maintenance, recovery, reconfiguration, adjustment of software, such a possibility is provided without decreasing of protection efficiency against unauthorized access.

Dependability Measures

Dependability measures define reliability, maintainability and durability of I&C systems and their components.

Reliability is standardized and estimated for the main functions, performed by I&C systems, SHC and peripheral equipment, and for components of I&C systems (except software) and removable component parts of SHC and peripheral equipment.

Failure criteria and reliability measures are determined considering function character (continuous or discrete) and type of possible failures. Continuous functions are monitoring, achieving, display, register (analogue) and regulation, discrete – warning, digital register, protection, limitation, interlocking, discrete and remote control.

Criteria of continuous function failures may be non-compliance, inaccurate meeting or violation of specified requirements for characteristics of performed function; as a reliability measures mean time between failures (MTBF) is taken. For discrete functions failure criteria are nonoperation (a failure type, where an output signal is absent, despite occurrence of conditions specified for its generation) and false operation (identified by availability of an output signal without conditions for its generation). As a reliability measures for “false operation” failures, failure flow parameter is taken, for “nonoperation” failures availability factor is standardized. For one and the same function several types of failures can be defined, which differ by cause of occurrence and / or effects, which they cause; in these cases failure criteria and reliability measures are determined individually for each type of failures.

Required value of reliability measures of each function is determined on agreement between a designer of I&C system (developer of SHC or peripheral equipment) and NPP (customer), in this case function category is considered. Values of these measures for functions, performed by updated or new I&C systems and SHC, are usually significantly exceed measures of the best prototypes, earlier operated in NPP.

During standardization and estimation of reliability function, reliability of all devices, taking part in its performance (including peripheral equipment, removable component parts of SHC, data transmission facilities and connecting lines, power sources, etc.) is considered. For this purpose failure criteria and required values of reliability measures for devises, used in the I&C system, are regulated. Failure criterion is non-compliance, inaccurate meeting or non-conformance of specified properties of at least one of required functions of device, this fact required its recovery or substitution. Reliability measures for devices, restored *directly on operating site*, is a MTBF or failure intensity, for non - restorable devices – mean time to first failure. Required values of reliability measures are determined for operationing conditions. Aging, deterioration, common cause failures, including software failures and personnel errors, are considered in case of availability of approved methods and initial data, which allow numerically estimate their probability and influence to reliability.

Maintainability is standardized and estimated for devices recoverable on operating site. Maintainability measures is a mean time to repair (MTTR), required for detection of inoperative component part of restorable (usually operating sand-alone) device, carrying out of preparatory operations (mounting of bypasses, disconnection of circuits, etc), replacement of inoperative component part to reserve and further checking of operation accuracy of the I&C system, SHC or device, execution of required final operations - recovery of circuits, removal of bypasses, etc. (MTTR does not include delays required for call and arrival of repair personnel, delivery of operable component part on an operating site of the device, paper work before and after recovery competition). Required values of MTTR are determined by agreement between a designer of the I&C system (developer of SHC or peripheral equipment) and NPP (customer) for all recoverable devices, taking part in performance of category A and B functions. They are usually supplemented with qualitative requirements for diagnostic, testability, checking automation, etc.

Design estimate of reliability and maintainability of SHC and peripheral equipment are executed till their procurement to the customer on the basis of estimations and / or results of reliability tests. Reliability and maintainability of main functions of the I&C system are preliminary calculated on the basis of data of components' reliability, participating in their performance, and main clarify by results obtained during trial operation.

Durability is standardized for I&C systems, SHC and peripheral equipment. As durability measure used mean life, defining time after which updating of the I&C system, replacement of SHC and / or peripheral equipment are executed, or a decision about possibility to continue operation within a new regulated period is made and agreed in accordance with the established procedure.

Mean life of new and updated I&C systems and SHC – are not less than 30 years. Within this period replacement of component parts of SHC and / or peripheral equipment, for which a mean life restricted by their suppliers is exceeded (not less than 15 years) is allowed.

Technical Diagnostic

Internal ("embedded") technical diagnostic facilities automatically control technical state and detect operability failures of removable component parts and redundant channels of SHC, peripheral equipment, command and signal transmission lines. Technical state control is executed after energization, continuously during operation and periodically.

After energization of SHC automatic checking is executed:

- Compliance of composition and configuration to design characteristics.
- Compliance of loaded software version to composition and configuration of SHC.
- Absence of distortions of in programs and data in read-only memory.
- Connection of all standard connectors.
- Up state of component parts of SHC.
- Operability of signal and command transmission circuits if it is possible.
- Accuracy of data transmission.
- Accuracy of exchange of messages between component parts of SHC with adjacent SHCs in a composition of the same and / or another I&C system.

SHC is considered operable and can be used as intended without any restrictions only after elimination of all defects detected during monitoring. Before elimination of defects a possibility and conditions of use of SHC as intended, required restrictions ad time, during which operability should be recovered, are regulated in Technical Specification on Safe Operation.

In the process of SHC operation, related to 2(A) and 3(B) safety class, continuous automatic control is performed for:

- Voltage of main and redundant power supply.
- Operability of transmission circuits of signals and commands.
- Reliability of analog and discrete input signals.
- Accuracy of operation of all component parts of SHC.
- Absence of errors during data exchange between component parts of SHC.
- Absence of errors in messages, received from other SHCs.
- Absence of software failures, causing termination of function performance.
- Other features (temperature rise and / or smoke in the operating stand-alone component parts of SHC, state of remote control circuits, operability of diagnostic hardware, etc.)

By agreement between the developer of SHC and operating organization or customer, automatic check of SHC, related to 3(C) safety class, can be performed to a lesser extent. Possibility and conditions of further use of SHC as intended in case of detection of defects, required restrictions and time period, within which operability of SHC should be recovered, are regulated in Technical Specification on Safe Operation.

After start-up and during the operation of peripheral equipment, related to 2(A) and 3(B) safety class, automatic check of operability (operation accuracy) is performed by use of built-in tests, provided by developers of these products (for peripheral equipment, related to 3(C) safety class, automatic check of operability is allowed after power-up).

If during check of technical state after start-up or during failure of, at least, one SHC or safety important peripheral equipment is detected, a relevant warning signal is automatically generated for personnel that monitors the state and provides maintenance and restoration of the I&C system. Information on time, occurrence and type of detected failure is achieved and displayed (automatically or on call) in the form that allows eliminating the failure in the shortest possible time. Visual and audible warning (general failure alarm) is automatically generated for operational personnel in the в main control room if operability failure prevents performing main function(s) of SHC or peripheral equipment of 2(A) or 3(B) safety class.

Performance of continuous automatic check during the operation, search of operability failures and generation of warnings, archiving and display of diagnostic information and failures of built-in diagnostic facilities do not have an influence on performance of main safety important functions of the I&C system.

Periodic check covers inspection of those components and properties of the I&C system, for which continuous automatic check during operation is impossible, unreasonable or not provided. Periodic check is performed within a whole period of operation of the I&C system – during the regulated maintenance (when power unit operates in operating modes) and each predictive and preventive maintenance (on a shutdown power unit).

During the regulated maintenance, the accuracy of implementation of each category A discrete function, sequentially simulating conditions, which require its performance, is checked. Deactivation for maintenance (periodic checking) of a redundant channel of SHC, participating in performance of emergency protection functions, is followed by automatic transmission and retention of each of its outputs in such a state that corresponds to initiation of commands of protective actions. In SHC, taking part in performance of other safety functions, each of outputs of deactivated redundant channel is automatically determined and retained in a state that corresponds to a lack of control and/or alarm command. Checking is executed without influencing actuating elements of technological equipment, it does not have any negative influence on operation and safety state of the unit, does not prevent functions execution by operational personnel and is finished by recovery of initial configuration of the I&C system (disconnection of mounted bypasses, return to previous set-points, etc.).

During predictive and preventive maintenance of power unit inspections cover all components, participating in performance of required (main) functions of the I&C system, for example, for regulating function– from a sensor to an end actuating element of technological equipment, including connecting cables. In general during periodic control of the I&C system and predictive preventive maintenance of power unit the following is provided:

- Resistance measurement of electrical isolation and grounding.
- Checking of accuracy of function performance of each redundant channel and system in whole, including with real actuators.
- Calibration of measuring channels, checking of accuracy characteristics of control and alarm channels.
- Determination of lags of output signal (command) generation and/or their duration.
- Executions of other inspections according to operational documentation.

Inspections allow detecting hidden operability failures of components, which are not detected during continuous automatic control and tendencies of alteration (degradation) of quantitative characteristics (resistance of isolation and grounding, errors, time lags, etc.), which in future can lead to a function failure.

Built-in diagnostic facilities, certified service equipment and supporting software, delivered together with SHC, provide automation of supply test influences (input signals), register of caused by them responses (output signals), determination of quantitative characteristics and archiving results of periodic control that allows minimizing labour intensity and duration of provided inspections. Service equipment connects to an examined device without its dismounting and breaking of external connections. For checking of devices, access to which during power unit operation is complicated or impossible (for example, placed inside the containment), service equipment is located in safety area on a distance from an examined product.

RESISTANCE OF FUNCTIONS EXECUTION

General Characteristics

Peripheral equipment, SHC and their operating stand-alone component parts have to be resistant (immune) to external influencing factors (EIF), which can occur in places of their location and saved as long as required (further – working operating conditions) and also to violation of operation conditions considered in the design during a limited time period (further – limit conditions). Limit conditions can be caused, for example, by accidents in technological equipment, connection, disconnection, failures of ventilation system, conditioning, power supply, providing working operating conditions, abnormal natural phenomena (earthquake, strokes of lightning) or internal events (fire, flood). In general resistance and insensibility are provided:

- To temperature, humidity, barometric pressure, ionizing radiation, corrosion-active agents, dust (EIF environment).
- To vibrations, strokes, seismic effects (mechanical EIF).
- To double-current electric fields (electrical EIF).
- To water and solutions, which can affect devices in accidents and to decontamination fluids (EIF specific environments).
- To long-term deviations from nominal values and short-term variation of power supply (EIF power supply).

- To influences of electrical technical or electronic equipment and other sources of electromagnetic disturbances (electromagnetic EIF).

EIF of each type is generally characterized by a set of qualitative features and quantitative parameters, related to working and limit conditions (further – working and limiting values EIF).

For peripheral equipment, SHC and their operating stand-alone component parts the following is indicated:

- Low and / or high working values of all EIF, which guarantee device operability and reservation of its characteristics within a regulated service life.
- Allowed low and / or high limiting values of each EIF, which a device should have and can sustain within a certain time period, keeping operability and without irreversible degradation of specified properties.

Instead of working and limiting values EIF parameters of testing influences, simulating influence of these EIFs during factory tests, under which operation accuracy of peripheral equipment and SHC is checked, are usually specified. Accurate operation is usually understood as performance of all required functions, absence of spurious output signals and absence of spurious signals and maintenance of properties within the specified limits. Violation of operation correctness is considered errors in performing at least one function, deviation of any product property over the specified (allowed) limits, generation of false output signal, loss or misrepresentation of information in the memory, necessity of personnel interference for reload and / or restart of software.

Test results are estimated by the following criteria:

a. Operation correctness during and after influence.
b. Temporary violation of operation correctness during influence and automatic (without personnel interference) recovery of correct operation after termination of influence.
c. Temporary violation of operation correctness during influence and recovery of correct operation by personnel interference after termination of influence.
d. Violation of operation correctness due to a damage caused by an influence (requires recovery of a failed device).

Resistance (insensitivity) of peripheral equipment and SHC is determined by A criterion. Test results obtained by B, C and D criteria indicate non-compliance with requirements of EIF resistance or insensitivity.

During planning and execution of EIF resistance tests (insensitivity), the following rules are applied:

- For power supply, generation of input signals or commands, monitor of output (output signals) state other operating stand-alone component parts of the same SHC and/or simulators and measurement technologies (further – auxiliary equipment) are used.
- Auxiliary equipment and connecting cables should be EIF resistant and immune or protected from their influence.
- Tests are carried out under nominal parameters of input signals and values of all EIF (except the tested one), which meet normal test conditions.
- EIF resistance (insensitivity) of each type is sequentially checked (except resistance to environment humidity and to irrigation of water and solutions during simulation of emergency conditions).

- For SHC and peripheral equipment, composed of several operating stand-alone component parts, are usually put to the test influences individually.
- Checking is executed in each of the regulated operation modes (or in a mode, in a which an product is the most EIF sensitive of a particular type, provide it was preliminary specified).
- Test influence is repeated a required number of times within a sufficient time period to estimate operation correctness with a required validation.

Resistance to the Environment Influence

SHC and peripheral equipment are resistant to the expected working values of EIF environment (without time restrictions) and to limiting values of these EIF (within an expected maximal duration of their existence). Working and limiting values of EIF environment is determined by a group of operating conditions, containing in a peripheral equipment and SHC (Table 1).

Table 1. Groups of operating conditions

Location Area	Room Category	Group of Operation Conditions
Strict access area	Rooms inside containment	E.1.1
	Rooms of technological equipment	E.1.2
	Rooms of primary transducers	E.1.3
	Rooms of electrical equipment and SHC	E.1.4
Normal access area	Rooms of technological equipment	E.2.1
	Rooms of electrical equipment and SHC	E.2.2
	Rooms with air condition (MCR, ECR, etc.)	E.2.3

During checking of resistance to EIF of the environment, one is guided by test data about actual working values of these EIF in places of devices' location, estimation results of their limiting values, expected duration and frequency of their occurrence. In case of lack of such data one considers generalized working (Table 2) and limit (Table 3 and 4) values for relevant groups of operation conditions (sign "–" means that EIF values are not regulated).

Resistance to EIF of the environment is confirmed by results of tests for influences of temperature, humidity, barometric pressure, ionizing radiation. Degree of test hardness is determined for EIF of each type, considering a group of operation conditions, to which a tested device relates, on the basis of Table 5.

Parameters of test influences, simulating EIF of environment are defined on the basis of a degree of test hardness using Table 6.

Resistance to influence of absorbed dose rate and to absorbed rate of continuous low intensive ionizing γ-radiation is checked by an experimental method and / or analysis of reference information, defining resistance of applied materials and component parts. Resistance to impacts of corrosive agents and dust are not executes if it is guaranteed by the design, applied materials and component parts and also experience of analogue operation at NPPs of Ukraine.

Resistance to Mechanical Influences

SHC and peripheral equipment are resistant to expected working values of mechanical EIF (without a time restriction) and to limiting values of these EIF, occurred during earthquakes. Working values of mechanical EIF are determined by a group of location conditions, to which each operating stand-alone device, contained in peripheral equipment and SHC, is related (Table 7).

During checking of resistance to working values of mechanical EIF, one is guided by test data about actual values of these EIF in places of

Table 2. Generalized working values of EIF of environment

Type of EIF and Measurements Unit	**Working Values of EIF for a Group of Operation Conditions**						
	E.1.1	**E.1.2**	**E.1.3**	**E.1.4**	**E.2.1**	**E.2.2**	**E.2.3**
Temperature:							
low value, °C	15	15	15	15	15	15	18
upper value, °C	60	60	30	30	60	30	27
Humidity:							
low value, %	5	5	10	10	5	10	20
upper value:							
% (at 15-30 °C)	100	90	75	75	90	75	80
g / m^3 (at 30-60 °C)	36	32	–	–	32	–	–
Barometric pressure:							
low value, кPa	86	86	86	86	86	86	86
upper value, кPa	108	108	108	108	108	108	108
Ionizing γ-radiation (upper value):							
Specific absorption rate, mGy / h	**	0,9	0,15	0,03	0,12	0,004	–
absorbed rate within 10 years, Gy	10^5	80	13	2,7	10,5	0,35	–
Concentration of corrosive agents*							
(upper value), mGy / m^3							
sulfur dioxide	10	10	10	10	10	10	10
hydrogen	10	10	10	10	10	10	10
nitrogen dioxide	10	10	10	10	10	10	10
hydrogen fluoride	1	1	1	1	1	1	1
hydrogen chloride	1	1	1	1	1	1	1
ammonia	35	35	35	35	35	35	35
Dust concentration (upper value), mg / m^3:	1	1	1	1	1	1	–

* For groups of operation conditions E.1.2 and E.2.1 upper working values of concentrations of other corrosive agents can be additionally defined. ** In case of location outside of technological boxes 30 mGy / h, in boxes 3 Gy / h

devices' location and in case of their lack of such data – on the basis of generalized working values for a group of location conditions, to which the device is related (Table 8).

For devices, related to groups of location conditions P1.1, P1.2 and P1.3, requirements for resistance to working values of mechanical EIF are not standardized.

Resistance to mechanical EIF is confirmed by results of tests for influence of sinusoidal vibrations and mechanical shocks. Degree of test hardness is determined on the basis of a group of location conditions, to which a tested device relates, using Table 9.

Parameters of test actions for the specified degree of test hardness are chosen according to Table 10.

For each operating stand-alone device, contained in peripheral equipment and SHC, a category of earthquake resistance (I, II or III) is determined on the basis of a role of performed functions for safety and operability assurance during and / or after earthquake.

Table 3. Generalized limiting values of EIF of environment for the group of operation conditions E.1.1

Type of EIF and Measurements Unit	Limiting Values of EIF for a Mode				
	A	B	C	D	E
Temperature (upper value), °C	75	90	150	60	60
Rate of change of temperature (upper value),°C / h	5	10	20	–	–
Humidity (upper value at an upper temperature value), %	100	steam-gas mixture		–	–
Barometric pressure:					
low value, кPa	50	86	86	50	–
upper value, кPa	130	180	560	130	560
Ionizing γ-radiation:					
Specific absorption rate, Gy / h	1,0	1,0	10^3	1,0	–
absorbed rate, Gy	15,0	5,0	10^4	$0{,}7\cdot10^3$	–
Duration (upper value), h	15	5	10	720	24

Note. Conventional symbols of modes: A – violation of heat removal from containment; B – small leak; C – maximal leak; D – post-accident mode (effects of a small and maximal leak); E – checking of leak resistance

Table 4. Generalized limiting values of EIF of environment for groups of operation conditions E.1.2, E.1.3, E.1.4, E.2.1, E.2.2, E.2.3

Type of EIF and Measurements Unit	Working Values of EIF for a Group of Operation Conditions					
	E.1.2	E.1.3	E.1.4	E.2.1	E.2.2	E.2.3
Temperature (upper value), °C	75	50	50	75	50	40
Rate of change of temperature (upper value),°C / h	10	5	5	10	5	5
Humidity (upper value at an upper temperature value), %	steam-gas mixture		98*	100	98*	90
Barometric pressure (upper value), кPa	130	130	–	–	–	–
Mode duration, h	5	3	2	3	2	2

* Without moisture condensation Note. Limiting values of EIF are defined: - for groups E.1.2 and E.2.1 – leak of technological equipment; - for a group E.1.3 – line break from technological equipment to sensors; - for groups E.1.4 и E.2.2 – ventilation disconnection; - for a group E.2.3 – conditioning system failure

Table 5. Degrees of test hardness of resistance to EIF of environment

EIF Type	Degrees of Test Hardness for a Group of Operation Conditions						
	E.1.1	E.1.2	E.1.3	E.1.4	E.2.1	E.2.2	E.2.3
Temperature	4	3	2	2	3	2	1
Relative humidity	4	3	2	2	3	2	1
Barometric pressure	2	1	–	–	–	–	–
Ionizing radiation	4	3	2	1	2	1	–

Note. Sign “–“ means that tests are not executed

Table 6. Test values of EIF of environment

Type Of EIF And Measurements Unit	Test Values of EIF for Degrees of Test Hardness (see Table 5)			
	1	2	3	4
Air temperature (exposure time, h, not less):				
low, not more	15°C (6 h)	15°C (6 h)	15°C (6 h)	15°C (6 h)
upper, not less	40°C (6 h)	50°C (6 h)	75°C (6 h)	150°C (10 h)
Rate of change, not less	–	5°C / h	10°C / h	20°C / h
Relative humidity (exposure time, h, not less):				
low, at 15°C, not more	–	10% (24 h)	5% (24 h)	5% (24 h)
upper, at 30°C, not less	–	–	90% (72 h)	100% (72 h)
at 40°C, not less	90% (6 h)	–	–	–
at 50°C, not less	–	100% (6 h)	–	–
at 75°C, not less	–	–	100% (6 h)	–
at 150°C, not less	–	–	–	100% (6 h)
Barometric pressure (exposure time, h, not less):				
low, not more	–	50 кPa (24 h)	–	–
upper, not less	130 (5 h)	560 кPa (24 h)	–	–
Absorbed dose rate of ionizing radiation, not less	$0,3{\cdot}10^{-4}$ Gy / h	$1,5{\cdot}10^{-4}$ Gy / h	$9{\cdot}10^{-4}$ Gy / h	0,03 Gy / h* 3 Gy / h**

* Test value for products, located outside of technological boxes ** Test value for products, located inside of technological boxes Note. Sign “–“means that tests are not executed

Table 7. Groups of location conditions

Sources of Mechanical EIF	Group of Operation Conditions	Mounting Technique	Group of Location Conditions
Absent	Any	On building constructions	P.1.1
		On supporting constructions	P.1.2
		On technological equipment	P.1.3
Available	E.1.3, E.1.4, E.2.2	On building constructions	P.2.1
		On supporting constructions	P.2.2
	E.1.1, E.1.2, E.2.1	On building constructions	P.3.1
		On supporting constructions	P.3.2
		On technological equipment	P.3.3

Devices, participating in performance of those functions that should be initiated and / or performed during an earthquake (emergency reactor shutdown, interlocking of driven mechanisms, etc.) or directly after an earthquake (emergency reactor cooling, residual heat removal, automatic control of critical parameters, radiation environment control, etc.) relate to categories I earthquake resistance. Device, related to category I earthquake resistance, should be resistant to seismic EIF on a place of its location, caused by an earthquake that can occur on-site with a repeatability period of

Table 8. Generalized working values of mechanical EIF

Type of EIF and Measurements Unit	Values of Mechanical EIF for a Group of Location Conditions				
	P.2.1	P.2.2	P.3.1	P.3.2	P.3.3
Sinusoidal vibrations:					
upper value of displacement amplitude*, mm	0,75	1,5	3,5	3,5	7,5
upper value of acceleration amplitude**, m/sec^2	2	5	10	10	20
upper value of frequency, Hz	150	150	150	150	150
Relative duration, %	100	100	100	100	100
influence direction	Z	Z	Z	Z	X, Y, Z
Mechanical shock:					
upper value of peak acceleration, m/sec^2	40	40	70	70	70
shock impulse duration, msec	100	100	50	50	50
influence direction	Z	Z	Z	Z	X, Y, Z

* At frequencies lower than crossover frequency (9-10 Hz) ** At frequencies higher than crossover frequency Note. In the table the following conventional symbols are used: X – direction along the horizontal plane; Y - direction along the horizontal plane, perpendicular X; Z - direction along the vertical plane

Table 9. Degrees of test hardness for resistance to mechanical EIF

EIF Type	Degrees of Test Hardness for a Group of Location Conditions							
	P.1.1	P.1.2	P.1.3	P.2.1	P.2.2	P.3.1	P.3.2	P.3.3
Sinusoidal vibrations	–	–	–	1	2	3	3	4
Mechanical shock	–	–	–	1	1	2	2	3

Note. Sign "–" means that tests are not executed

every 10 000 years (further - maximum credible earthquake or MCE).

Devices, which didn't come into category I, relate to category II earthquake resistance if failures of performed functions, caused by an earthquake, can lead to power generation break (reactor power control, retention of technological parameters within specified limits, etc.). Device, related to category II earthquake resistance, should be resistant to seismic EIF on the place of its location, caused by an earthquake that can occur on-site with a repeatability period 1 in 500 years (further – design basis earthquake or DBE). Devices that cannot be related to categories I or II by the above specified criteria, relate to category III earthquake resistance. Earthquake resistance requirements for them are not regulated.

Seismic EIF on the place of device's location define response spectrum that considers a possible response of building and intermediate constructions to horizontal and vertical earth seismic vibrations, which can be filtered or intensified on the basis of typical for these constructions own vibration rate and damping.

Response spectrum is determined by calculation and / or modeling, taking into account:

Table 10. Test values of mechanical EIF

Type and Measurements Unit	Test Values of EIF for Degrees of Test Hardness (see Table 9)			
	1	2	3	4
Sinusoidal vibration				
displacement amplitude (in frequency rate 1 - 9 Hz), not less	0,75 mm	1,5 mm	3,5 mm	7,5 mm
acceleration amplitude (in frequency rate 9-150 Hz), not less	2,0 m / sec^2	5,0 m / sec^2	10 m / sec^2	20 m / sec^2
duration, not less	60 min	60 min	60 min	60 min *
influence direction	Z	Z	Z	X, Y, Z
Mechanical shocks				
peak shock acceleration, not less	40 m / sec^2	70 m / sec^2	70 m / sec^2	–
shock impulse duration	100 msec	50 msec	50 msec	–
shock impulse shape	sinusoid half-wave			–
period between shocks, not less	2,0 sec	2,0 sec	2,0 sec	–
number of shocks, not less	1000	1000	1000*	–
influence direction	Z	Z	X, Y, Z	–

* In each direction *Note.* In the table the following conventional symbols are used: X – direction along the horizontal plane; Y - direction along the horizontal plane, perpendicular X; Z - direction along the vertical plane

- Seismicity of NPP site (intensity level of MCE and DBE in points).
- Soil conditions in the site of unit on the basis of seismic microzoning information.
- Accelerograms of MCE and DBE, synthesized by statistic processing and analysis of a range of accelerograms of real earthquakes.
- Rate of own vibrations and damping parameters (damping factor or algorithmic decrement) of a building construction.
- Height of location and a mounting technique of device on a building supporting construction (ceiling, wall, column), intermediate construction (in a room, case, panel, board) or technological equipment (piping, pipeline valve, etc.)

In case of lack of results of calculation of modeling required response spectrum is determined on the basis of generalized values of seismic EIF (Table 11).

Required response spectrum is characterized by two horizontal and a vertical components acting simultaneously. Acceleration amplitudes in a vertical direction are accepted with a level 0,7 from the specified in Table 11.

Earthquake resistance of peripheral equipment and SHC is determined on the basis of test results, during which each of their operating standalone component parts are put under influence of sinusoidal vibration, simulating seismic EIF. Degree of test hardness is determined according to Table 12, depending on the specified intensity level of MCE and DBE, mounting technique and height, at which a device will be installed.

During tests a provided technique of device mounting is simulated, using parts, materials and technology specified in documentation.

Test influence is chosen according to Table 13 and controlled in the place of device mounting.

Test influence is simultaneously applied along three mutually orthogonal (two horizontal and vertical) directions. In case of lack of a required

Table 11. Generalized values of seismic EIF (required response spectrums)

*	Mounting Technique	Height, m	Acceleration Amplitude m /sec^2, at Frequency, Hz									
			0,5	1	2	3	4	5	6	10	15	30
Maximum Credible Earthquake (Average Repeatability 10 000 Years)												
VI	On building constructions	From 0 to 5 inclusive	0,1	1,5	1,9	1,9	1,9	1,9	1,9	1,9	1,5	0,8
		Over 5 to 10 inclusive	0,2	3,0	3,8	3,8	3,8	3,8	3,8	3,8	3,0	1,5
		Over 10 to 25 inclusive	0,4	5,7	7,2	7,2	7,2	7,2	7,2	7,2	5,7	3,0
		Over 25 to 35 inclusive	0,6	8,0	9,5	9,5	9,5	9,5	9,5	9,5	8,0	4,0
		Over 35 to 70 inclusive	0,8	9,8	12,4	12,4	12,4	12,4	12,4	12,4	9,8	4,9
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	0,2	3,0	3,8	3,8	3,8	3,8	3,8	3,8	3,0	1,5
		Over 5 to 10 inclusive	0,5	6,0	7,6	7,6	7,6	7,6	7,6	7,6	6,0	3,0
		Over 10 to 25 inclusive	0,9	11,4	14,5	14,5	14,5	14,5	14,5	14,5	11,4	5,7
		Over 25 to 35 inclusive	1,1	15,0	19,0	19,0	19,0	19,0	19,0	19,0	15,0	7,5
		Over 35 to 70 inclusive	1,5	19,8	24,7	24,7	24,7	24,7	24,7	24,7	19,8	9,9
VII	On building constructions	From 0 to 5 inclusive	0,2	2,4	3,0	3,0	3,0	3,0	3,0	3,0	2,4	1,2
		Over 5 to 10 inclusive	0.4	4,8	6,0	6,0	6,0	6,0	6,0	6,0	4,8	2,4
		Over 10 to 25 inclusive	0,8	9,2	11,4	11,4	11,4	11,4	11,4	11,4	9,2	4,6
		Over 25 to 35 inclusive	1,0	12,0	15,0	15,0	15,0	15,0	15,0	15,0	15,0	7,5
		Over 35 to 70 inclusive	1,3	15,6	19,5	19,5	19,5	19,5	19,5	19,5	15,6	7,8
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	0.4	4,8	6,0	6,0	6,0	6,0	6,0	6,0	4,8	2,4
		Over 5 to 10 inclusive	0,8	9,6	12,0	12,0	12,0	12,0	12,0	12,0	9,6	4,8
		Over 10 to 25 inclusive	1,6	18,3	22,8	22,8	22,8	22,8	22,8	22,8	18,3	9,2
		Over 25 to 35 inclusive	2,0	24,0	30,0	30,0	30,0	30,0	30,0	30,0	24,0	12,0
		Over 35 to 70 inclusive	2,6	31,2	39,0	39,0	39,0	39,0	39,0	39,0	31,2	15,6
VIII	On building constructions	From 0 to 5 inclusive	0,3	4,0	5,0	5,0	5,0	5,0	5,0	5,0	4,0	2,0
		Over 5 to 10 inclusive	0,6	8,0	10,0	10,0	10,0	10,0	10,0	10,0	8,0	4,0
		Over 10 to 25 inclusive	1,2	14,4	19,0	19,0	19,0	19,0	19,0	19,0	14,4	7,6
		Over 25 to 35 inclusive	1,5	20,0	25,0	25,0	25,0	25,0	25,0	25,0	20,0	10,0
		Over 35 to 70 inclusive	2,0	26,0	32,5	32,5	32,5	32,5	32,5	32,5	26,0	13,0
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	0,6	8,0	10,0	10,0	10,0	10,0	10,0	10,0	8,0	4,0
		Over 5 to 10 inclusive	1,2	16,0	20,0	20,0	20,0	20,0	20,0	20,0	16,0	8,0
		Over 10 to 25 inclusive	2,3	30,4	38,0	38,0	38,0	38,0	38,0	38,0	30,4	15,2
		Over 25 to 35 inclusive	3,0	40,0	50,0	50,0	50,0	50,0	50,0	50,0	40,0	20,0
		Over 35 to 70 inclusive	3,9	52,0	65,0	65,0	65,0	65,0	65,0	65,0	52,0	26,0

continued on following page

Table 11. Continued

*	Mounting Technique	Height, m	Acceleration Amplitude m /sec^2, at Frequency, Hz									
			0,5	**1**	**2**	**3**	**4**	**5**	**6**	**10**	**15**	**30**
IX	On building constructions	From 0 to 5 inclusive	0,5	5,6	7,0	7,0	7,0	7,0	7,0	7,0	5,6	2,8
		Over 5 to 10 inclusive	1,0	11,2	14,0	14,0	14,0	14,0	14,0	14,0	11,2	5,6
		Over 10 to 25 inclusive	1,9	21,3	26,6	26,6	26,6	26,6	26,6	26,6	21,3	10,7
		Over 25 to 35 inclusive	2,5	28,0	35,0	35,0	35,0	35,0	35,0	35,0	28,0	14,0
		Over 35 to 70 inclusive	3,3	36,4	45,5	45,5	45,5	45,5	45,5	45,5	36,4	18,2
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	1,0	11,2	14,0	14,0	14,0	14,0	14,0	14,0	11,2	5,6
		Over 5 to 10 inclusive	2,0	22,4	28,0	28,0	28,0	28,0	28,0	28,0	22,4	11,2
		Over 10 to 25 inclusive	3,8	42,6	53,2	53,2	53,2	53,2	53,2	53,2	42,6	21,3
		Over 25 to 35 inclusive	5,0	56,0	70,0	70,0	70,0	70,0	70,0	70,0	56,0	28,0
		Over 35 to 70 inclusive	6,5	72,8	91,0	91,0	91,0	91,0	91,0	91,0	72,8	36,4
Design Basis Earthquake (Average Repeatability 500 Years)												
V	On building constructions	From 0 to 5 inclusive	–	–	–	–	–	–	–	–	–	–
		Over 5 to 10 inclusive	–	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,2
		Over 10 to 25 inclusive	–	0,5	0,6	0,6	0,6	0,6	0,6	0,6	0,5	0,3
		Over 25 to 35 inclusive	–	0,6	0,8	0,8	0,8	0,8	0,8	0,8	0,6	0,3
		Over 35 to 70 inclusive	–	0,8	1,0	1,0	1,0	1,0	1,0	1,0	0,8	0,4
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	–	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,2
		Over 5 to 10 inclusive	–	0,5	0,6	0,6	0,6	0,6	0,6	0,6	0,5	0,3
		Over 10 to 25 inclusive	–	1,0	1,2	1,2	1,2	1,2	1,2	1,2	1,0	0,5
		Over 25 to 35 inclusive	–	1,2	1,5	1,5	1,5	1,5	1,5	1,5	1,2	0,6
		Over 35 to 70 inclusive	–	1,6	2,0	2,0	2,0	2,0	2,0	2,0	1,6	0,8
VI	On building constructions	From 0 to 5 inclusive	–	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,2
		Over 5 to 10 inclusive	–	0,5	0,6	0,6	0,6	0,6	0,6	0,6	0,5	0,3
		Over 10 to 25 inclusive	–	1,0	1,2	1,2	1,2	1,2	1,2	1,2	1,0	0,5
		Over 25 to 35 inclusive	–	1,2	1,5	1,5	1,5	1,5	1,5	1,5	1,2	0,6
		Over 35 to 70 inclusive	–	1,6	2,0	2,0	2,0	2,0	2,0	2,0	1,6	0,8
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	–	0,5	0,6	0,6	0,6	0,6	0,6	0,6	0,5	0,3
		Over 5 to 10 inclusive	–	1,0	1,2	1,2	1,2	1,2	1,2	1,2	1,0	0,5
		Over 10 to 25 inclusive	–	2,0	2,4	2,4	2,4	2,4	2,4	2,4	2,0	1,0
		Over 25 to 35 inclusive	0,2	2,4	3,0	3,0	3,0	3,0	3,0	3,0	2,4	1,2
		Over 35 to 70 inclusive	0,3	3,2	4,0	4,0	4,0	4,0	4,0	4,0	3,2	1,6

continued on following page

Table 11. Continued

*	Mounting Technique	Height, m	Acceleration Amplitude m /sec^2, at Frequency, Hz									
			0,5	1	2	3	4	5	6	10	15	30
VII	On building constructions	From 0 to 5 inclusive	–	0,5	0,6	0,6	0,6	0,6	0,6	0,6	0,5	0,3
		Over 5 to 10 inclusive	–	1,0	1,2	1,2	1,2	1,2	1,2	1,2	1,0	0,5
		Over 10 to 25 inclusive	–	2,0	2,4	2,4	2,4	2,4	2,4	2,4	2,0	1,0
		Over 25 to 35 inclusive	0,2	2,4	3,0	3,0	3,0	3,0	3,0	3,0	2,4	1,2
		Over 35 to 70 inclusive	0,3	3,2	4,0	4,0	4,0	4,0	4,0	4,0	3,2	1,6
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	–	1,0	1,2	1,2	1,2	1,2	1,2	1,2	1,0	0,5
		Over 5 to 10 inclusive	–	2,0	2,4	2,4	2,4	2,4	2,4	2,4	2,0	1,0
		Over 10 to 25 inclusive	0,3	4,0	4,8	4,8	4,8	4,8	4,8	4,8	4,0	2,0
		Over 25 to 35 inclusive	0,4	4,8	6,0	6,0	6,0	6,0	6,0	6,0	4,8	2,4
		Over 35 to 70 inclusive	0,5	6,4	8,0	8,0	8,0	8,0	8,0	8,0	6,4	3,2
VIII	On building constructions	From 0 to 5 inclusive	–	1,0	1,2	1,2	1,2	1,2	1,2	1,2	1,0	0,5
		Over 5 to 10 inclusive	–	2,0	2,4	2,4	2,4	2,4	2,4	2,4	2,0	1,0
		Over 10 to 25 inclusive	0,3	4,0	4,8	4,8	4,8	4,8	4,8	4,8	4,0	2,0
		Over 25 to 35 inclusive	0,4	4,8	6,0	6,0	6,0	6,0	6,0	6,0	4,8	2,4
		Over 35 to 70 inclusive	0,5	6,4	8,0	8,0	8,0	8,0	8,0	8,0	6,4	3,2
	On intermediate constructions or technological equipment	From 0 to 5 inclusive	–	2,0	2,4	2,4	2,4	2,4	2,4	2,4	2,0	1,0
		Over 5 to 10 inclusive	0,3	4,0	4,8	4,8	4,8	4,8	4,8	4,8	4,0	2,0
		Over 10 to 25 inclusive	0,6	8,0	9,6	9,6	9,6	9,6	9,6	9,6	8,0	4,0
		Over 25 to 35 inclusive	0,8	9,6	12,0	12,0	12,0	12,0	12,0	12,0	9,6	4,8
		Over 35 to 70 inclusive	1,0	12,8	16,0	16,0	16,0	16,0	16,0	16,0	12,8	6,4

* Earthquake intensity in points

influence for this test equipment, a simultaneous influence along two (one of horizontal and vertical) directions is executed, at this time acceleration amplitudes in a horizontal direction are increased in 1,4 times comparing to the specified one in Table 13. Acceleration amplitude at every frequency is suggested to choose 15% over the specified in Table 13 to guarantee coverage of the required response spectrum of test values. Hold time at each frequency - not less than 10 sec.

During and / after test influences, corresponding to maximum credible earthquake, also those EIF are simulated, which can occur in emergency situations or accidents, caused by such an earthquake and have a negative impact on device earthquake resistance. For consideration of possible factors of mechanical aging, devices of category I earthquake resistance before resistance tests for maximum credible earthquake are put under test influences not less than 5 times, which simulate a design basis earthquake.

Devices of category I and II earthquake resistance should not have primary frequencies of own vibrations (resonant frequencies) in a range from 0,5 to 30 Hz. The devices, their racks and mounts, provided by documentation, should be resistant to overthrow under static force, applied to the center of mass, and equal to the product of maximal acceleration with the device mass.

Table 12. Degrees of test hardness of earthquake resistance

*	Mounting Technique	Degrees of Test for Installation Height, m				
		From 0 to 5 Inclusive	**Over 5 to 10 Inclusive**	**Over 10 to 25 Inclusive**	**Over 25 to 35 Inclusive**	**Over 35 to 70 Inclusive**
For Devices of Category I Earthquake Resistance						
VI	On building constructions	3	4	5	6	6
	On intermediate constructions	4	5	6	7	7
	On technological equipment	4	5	6	7	7
VII	On building constructions	4	5	6	6	7
	On intermediate constructions	5	6	7	7	8
	On technological equipment	5	6	7	7	8
VIII	On building constructions	5	6	7	7	8
	On intermediate constructions	6	7	8	8	9
	On technological equipment	6	7	8	8	9
IX	On building constructions	5	6	7	8	8
	On intermediate constructions	6	7	8	9	9
	On technological equipment	6	7	8	8	9
For Devices of Category II Earthquake Resistance						
V	On building constructions	–	1	2	2	2
	On intermediate constructions	1	2	3	3	3
	On technological equipment	1	2	3	3	3
VI	On building constructions	1	2	3	3	3
	On intermediate constructions	2	3	4	4	4
	On technological equipment	2	3	4	4	4
VII	On building constructions	2	3	4	4	4
	On intermediate constructions	3	4	5	5	5
	On technological equipment	3	4	5	5	5
VIII	On building constructions	3	4	5	5	5
	On intermediate constructions	4	5	6	6	6
	On technological equipment	4	5	6	6	6

* Earthquake intensity in points

Immunity to Electrical Action

Peripheral equipment, SHC and their operating stand-alone component parts should be immune to the influence of electric EIF (low-frequency electric fields) in working operation conditions.

Actual or expected working values of intensity of low-frequency electric fields in places of location of these devices are determined on the basis of experimental and/ or design data, in case of their lack– on the basis of generalized working parameters of electric EIF (Table 14).

Immunity to electric EIF is defined on the basis of test results, during which operating stand-alone component parts are sequentially put under test influences, simulating electric low-frequency field, possible in working operating conditions. Parameters of test influences are chosen according to Table 15.

Table 13. Test influences simulating seismic EIF

Degrees of Test Hardness	Acceleration Amplitude along a Horizontal Plane, m /sec^2, at Frequency									
	0,5 Hz	1 Hz	2 Hz	3 Hz	4 Hz	5 Hz	6 Hz	10 Hz	15 Hz	30 Hz
1	–	0,4	0,5	0,5	0,5	0,5	0,5	0,5	0,4	0,2
2	–	0,8	1,0	1,0	1,0	1,0	1,0	1,0	0,8	0,4
3	0,1	1,5	2,0	2,0	2,0	2,0	2,0	2,0	1,5	0,8
4	0,2	3,0	4,0	4,0	4,0	4,0	4,0	4,0	3,0	1,5
5	0,5	6,0	8,0	8,0	8,0	8,0	8,0	8,0	6,0	3,0
6	1,0	12,0	16,0	16,0	16,0	16,0	16,0	16,0	12,0	6,0
7	2,0	24,0	32,0	32,0	32,0	32,0	32,0	32,0	24,0	12,0
8	4,0	48,0	64,0	64,0	64,0	64,0	64,0	64,0	48,0	24,0
9	8,0	96,0	96,0	96,0	96,0	96,0	96,0	96,0	96,0	48,0

Note. Acceleration amplitude in a vertical direction – not less than 70% from the specified

Table 14. Generalized working values of electric EIF

Type of EIF and Measurements Unit	Working Values of Electric EIF for a Group of Operation Conditions						
	E1.1	E1.2	E1.3	E1.4	E2.1	E2.2	E2.3
Electric field intensity, кV / m	5	5	5	–	5	–	–
Electric field frequency, Hz	50	50	50	–	50	–	–

Note. 1. Phase of electric field regarding voltage of feeding alternating current and direction of intensity vector can be any 2. Sign "–" - is not regulated

Table 15. Test values of electric EIF

Type of EIF and Measurements Unit	Test Values for a Group of Operation Conditions						
	E1.1	E1.2	E1.3	E1.4	E2.1	E2.2	E2.3
Electric field intensity, кV / m, not less	5	5	5	–	5	–	–
Electric field frequency, Hz	50	50	50	–	50	–	–

Note. 1. Phase of electric field regarding voltage of feeding alternating current, feeding product, - 0º; 90º; 270º (sequentially) 2. Direction of intensity vector of electric field – sequentially along each of three orthogonal planes 3. Sign "–" means that tests are not executed

Resistance to Impacts of Special Influences

Peripheral equipment and operating stand-alone component parts of SHC related to a group of operation conditions E1.1, E1.2, E1.3, E1.4 or E2.1 are resistant to:

- Irrigation of water and solutions, which composition, temperature, direction and duration of influence are determined on the basis of analysis of possible accident effects in places of devices' location.
- Influence of decontamination fluids, chemical compositions and mass fractions of each components, which are agreed with an operating organization or customer.

In case of availability of automatic gas fire-fighting in rooms, where devices, related to safety class 2(A), are located, they should be resistant to reagent influence, filling a room in case of fire fighting system actuation (type of applied reagent is agreed with an operative organization or customer).

Immunity to Change of Power Parameters

Safety important I&C systems and SHC receive primary power supply from a circuit of own needs of the unit with single- or three-phase current with a nominal voltage of 220 V or 380 / 220 V and frequency of 50 Hz. Power supply of peripheral equipment and operating stand-alone component parts of SHC is directly performed from the circuit of own needs or from secondary feed sources, contained in the I&C system and / or SHC. The I&C systems and SHC include facilities for distribution and protection of power circuits and if required uninterruptable power sources.

Peripheral equipment and SHC are immune to long-term deviations of voltage of primary power supply, short-term changes and fluctuations of voltage, power interruption, long- and short-term changes of supply frequency, which are possible in working and limit operation conditions. Products that obtain secondary power from sources, contained in the I&C system and SHC, are immune to changes in parameters of primary power supply of these sources.

Immunity is estimated on the basis of test results, during which the following rules are followed additionally to general provisions in this chapter:

- All operating stand-alone component parts of peripheral equipment and SHC, receiving power from one source, are tests simultaneously.
- Points of application of test influences are power ports – terminal screw, clamps, connectors and other device constructive elements, defining its physical borders from a circuit of own needs (device can have one or several power ports).
- If a device has several mutually redundant power ports, test influences are supplied by turns to each port, at this time other ports should be disconnected from the circuit.
- Standards and rules for estimation of resistance to changes of power parameters, testing methods and estimation criteria correspond to the ones specified in NP, 2000 and State standards of Ukraine, identical to international standards IEC, 2002a; IEC 2002c; IEC 2004.

Immunity to Electromagnetic Disturbances

I&C systems, peripheral equipment and SHC are immune to electromagnetic EIF (electromagnetic disturbances), which influence or can influence them in working and limit operating conditions:

- Disturbances from electrostatic discharges.
- Disturbances from radio frequency electromagnetic radiation.
- Disturbances from rapid transient processes/ packages of impulses.
- Disturbances from power and current spikes.
- Conductive disturbances, brought by radiofrequency fields.
- Disturbances from magnetic fields of circuit frequency.
- Disturbances from impulse magnetic fields.
- Disturbances from damped oscillatory magnetic field.
- Oscillatory damped disturbances.
- Conductive asymmetric disturbances in a range from 0 Hz to 150 кHz.
- Disturbances in ground lines.

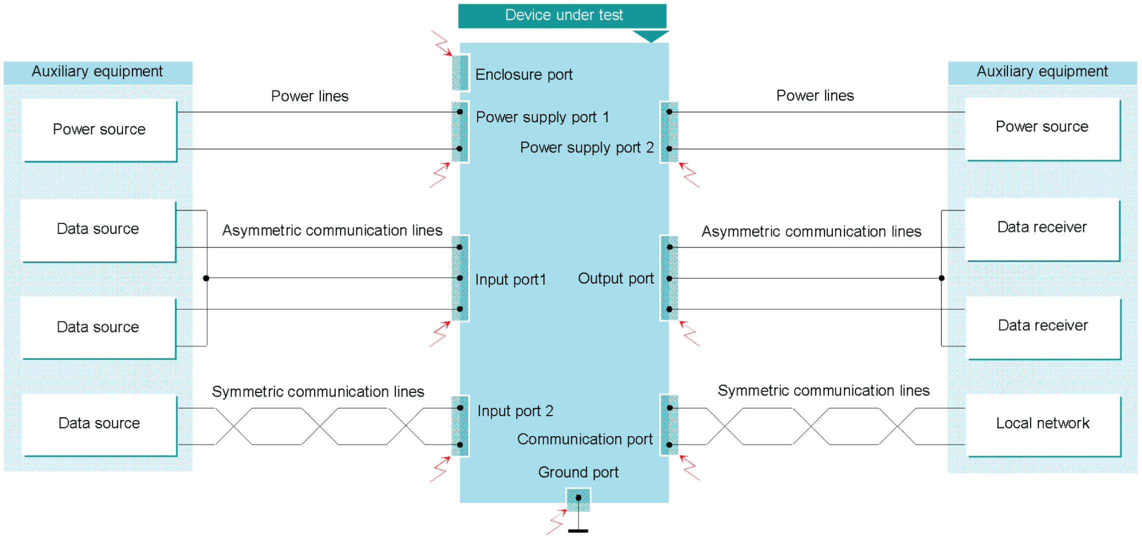
Required immunity to disturbances is provided in the process of design of I&C systems, development, manufacturing and mounting of peripheral equipment and SHC and is kept during operation due to creation and support of a proper electromagnetic environment in places of their location.

Immunity to disturbances is standardized by determination of parameters of test influences, simulating disturbances of each type and also places of their application and ways of brining test influences, at which tested peripheral equipment and SHC should operate properly. Places of application of test influences, simulating disturbances, are terminal screw, clamps, connectors and other device constructive elements, defining its physical borders with environment (further – ports, see Figure 5):

- **Power Port:** In places of connection of two or more wires from one power source to a device.
- **Input Port:** In places of connection of two or more wires from one or several interconnected sources of input signals to a device.
- **Output Port:** In places of connection of two or more wires to a device, connecting it with one output receiver.
- **Communication Port:** In places of device connection to one communication channel or one local network.
- **Ground Port:** In places of device connection to a system of protective or, if available, - signal ground (signal ground port is determined as a place, in which isolated from the shell of input, output and/or communication circuits are gathered for connection to the ground major node).
- **Enclosure Port:** On outer surface of device enclosure and nonconductive elements connected with and on screens of external cables electrically connected with a shell.

For estimation of immunity to electromagnetic disturbances tests are executed, during which peripheral equipment and operating stand-alone component parts of SHC are put under test influences, simulating actions of disturbances of

Figure 5. Places of application of test influences, simulating disturbances

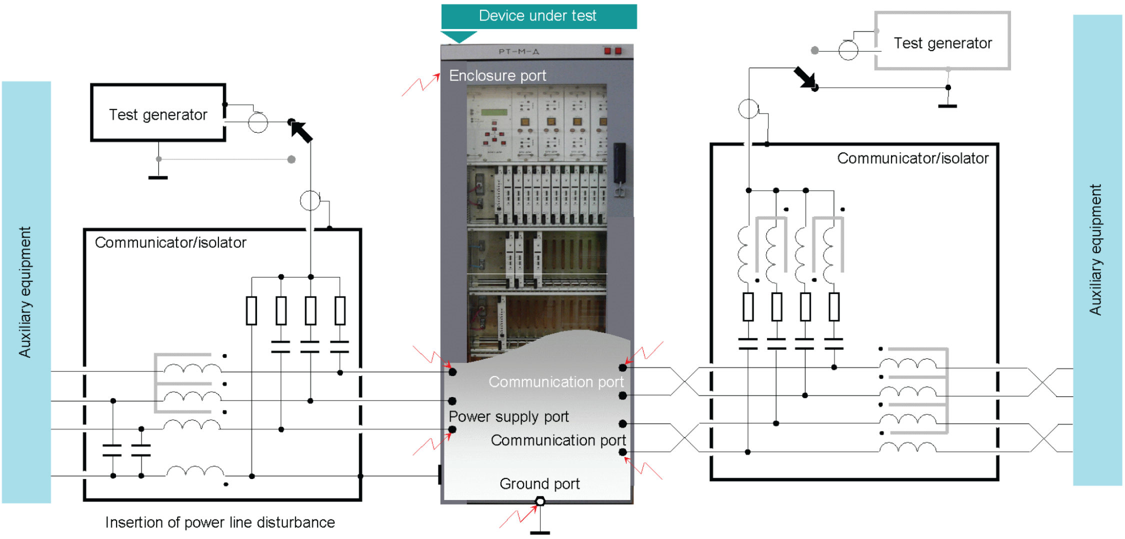


each type that are possible in working and limit operation conditions. In general, test influences are applied to circuits, connected to the power port(s) of direct and alternating current; to unsymmetrical and / or symmetrical connecting lines, connected to input, output, communication ports; to ports of protective and (if available) signal ground and to a enclosure port (see Figure 6).

During tests of immunity to electromagnetic disturbances, the following rules are followed additionally to general provisions:

- Electromagnetic environment in rooms, where tests are executes, should not influence their results.
- Tests are executed by turn regarding each type of disturbances specified in technical specification (immunity to a simultaneous activity of disturbances of several types is not checked).
- Device location, types and length of connecting cables should, when applicable, meet real operation conditions (cables, containing or provided in technical documentation of SHC and peripheral equipment, should be used).
- Test influences are allowed to be generated simultaneously on several operating standalone component parts of SHC, interconnected by electric communication lines (length not less than 1 m) and / or non-electric communication lines.
- If a device has several power, ground, input, output and communication ports, test influences are generated on each of them individually.
- For devices that have a significant (more than 5) number of identical ports or ports with a considerable number of connecting lines with an approval of a limited number of such ports (lines), which are the most sensitive to disturbances of such a type.
- Degree of test hardness is chosen considering electromagnetic environment in places of actual and expected location of devices during operation (qualitative features, by

Figure 6. Example of workplace arrangement for execution of tests of disturbance immunity



which an electromagnetic environment is classified, are presented in NP, 2000; Rozen, 2007; Rozen, 2008).

- When selecting a degree of test hardness, those (and only those) features of electromagnetic environment, which can be a cause of occurrence and have a significant influence on intensity of disturbances of that type, towards which tests are executed, are considered.

Standards and rules of noise immunity estimation, test methods and criteria of result estimation meet international standards IEC 2001a - IEC 2001g; IEC, 2002a – IEC, 2002c; IEC 2005b; IEC, 2006a and identical with them State standards of Ukraine (Rozen, 2007, Rozen, 2008).

Resistance to Failures of Elements

Safety important I&C systems and SHC are designed (developed) in such a way that they could continue operation with preliminary determined behavior in case of single failures of their elements and / or element failures in adjacent I&C systems and in channels, through which information is obtained from these systems. Each of main functions of the I&C system and SHC is performed and meet specified requirements in case of failure of any elements of the same system (SHC), participating in functions execution of lower category.

Failures of elements in primary and secondary power supply systems do not influence functions of the I&C system (SHC). If such failures lead to short-term power break, not exceeding a specified time period, they do not influence performance of category A and B functions; performance of category C functions is continued in a previous mode after power supply recovery.

Resistant to failures of elements is provided in I&C systems and SHC of 2(A) and 3(B) safety classes:

- Adequate supplies of calculating and other resources (inputs, outputs, memory, power supply, etc.)
- Redundancy of components of I&C systems and component parts of SHC, performing category A and B, and equipment and connecting lines, which are used for transmission of signals and messages between them and reception of required information from other systems.
- Availability of devices that can detect deviations from a determined behavior and automatically recover normal operation (for example, timer, executing restart in case of program circularity or temporary loss of input data).
- Availability of technical diagnostic facilities, which provide continuous checking of a technical state and allow promptly detecting operation failures of component parts, which can lead to a failure during initiation of a discrete function.
- A possibility of algorithm restructuring, which allows recovering operation of failed elements in a normal mode or transferring to a preliminary provided standby mode, for example, in case of unreliability of received data or a loss of input data that is impossible to eliminate.

For assurance of resistance to failures of information sources or connecting lines:

- Validity of input analog signals (for example, when this signal is staging in working range what have defined preliminary for designate parameter) is checked and unreliable data are automatically eliminated.
- For formation, transmission and input of data about the state of a controlled object, two-beat signals are used instead of one-bit binary signals, when logical levels 01 and

10 are interpreted as two different states of an object (for example, connected and disconnected), at this time logical levels 00 and 11 indicate an error of a signal source or a damage of a connecting line.

- For reception of commands of remote control from operational personnel keys with three states, connected with a three- or four-wired scheme in such a way that any command is generated during a simultaneous opening of a control circuit (closed at a mid position of the key) and closed control circuits in one of two extreme positions of the key, are used.

For assurance of resistance to failures of elements in channels of digital message transmission communication protocols, which are able to detect and correct errors in received messages are applied, and/or data reliability recovery, used for further processing in each of redundant channels, is provided.

QUALITY OF FUNCTIONS EXECUTION

Accuracy

Accuracy requirements are regulated for measuring channels of the I&C system and SHC, which display, register, archive and / or transmit numerical values of physical quantities in allowed for them units, for control channels (protection, interlocking, regulation) and alarm, and also (on agreement between a developer and operating organization or a customer) for components of the I&C system and component parts of SHC, forming measuring channels, control and alarm channels.

During standardization and estimation of accuracy the following rules are followed:

- Main safety important technological parameters are preferably monitored by a direct measuring method rather than calculated on the basis of measured values of other parameters (indirect measurements).
- When choosing a measurement range for each monitored parameter, a possibility of exceeding a range of working values of this parameter in emergencies and accidents is considered.
- If for a satisfactory coverage of all range of a monitored parameter more than one sensor is required, a proper overlapping of adjacent measurement ranges and automatic switching of these sensors are provided in order that saturation or corruption influence on range boundaries does not prevent reception of results with a required accuracy.
- In case of inoperability or removal from operation of one of a redundant measuring channel (control or alarm channel), other channels should meet specified accuracy requirements.
- Measuring channels, control and alarm channels, in which redundancy of component parts is provided, should meet specified accuracy requirements in case of failure of any of these component parts.

Accuracy of measuring channels is specified in form of metrological characteristics of these channels, to which a measurement range, conversion function, error characteristics are related. Error characteristics of a measuring channel are standardized:

- Allowed absolute, relative or conventional error in working (on agreement between the developer and the operating organization or a customer – limit) operation conditions.

- Allowed main (absolute, relative or conventional) error under normal test conditions and allowed additional errors, which can be caused by a change of each EIF in a range of specified for it working or limiting values.

Conventional error of a measuring channel is calculated as a ratio of an absolute error to a range of monitored parameter change. Absolute error is determined as a difference between a measured and actual value of a monitored parameter, where a measured one is considered a parameter value: directly obtained for a data base; displayed or registered in a digital or analog form; calculated by an output signal; transmitted in an output digital signal (message). For the I&C system as an actual value of a monitored parameter a result of its estimation by use of measurement facilities is accepted, for SHC – by a measured value of a proper analog Input signal, considering a nominal static characteristic of the signal source (sensor, normalizing transducer, etc.).

Accuracy requirements of measuring channels are established by agreement between the developer and operating organization (customer), where metrological characteristics of updated I&C systems and, first of all, contained in them SHC, are usually significantly higher than previously operated ones had. Before commissioning, all measuring channels of the I&C system pass metrological certification according to requirements of state standards of Ukraine.

In grounded cases, instead of metrological characteristics of measuring channels, metrological characteristics of component parts, which are determined for assurance of a metrological compatibility of these component parts that allows defining metrological characteristics of measuring channels by a calculation method, can be regulated. Experimental estimation of metrological characteristics of component parts of measuring channels is executed during their development, after manufacturing and during operation.

Accuracy of alarm and control channels is specified in a form of accuracy characteristics of these channels in working and limit operation conditions. Accuracy characteristics include limits of an allowed absolute error of output and withdrawal of a command (output signal) and limits of allowed relative error of formation time lags and / or dwells if they are provided in algorithms of performance of control functions.

For the I&C system, an absolute error of output and withdrawal of a command (output signal) is determined as a difference between an actual value of a controlled parameter, caused the indicated action, and a specified value (set-point) of this parameter, under which such an action should be executed. For SHC during determination of an absolute error instead of a controlled parameter, values of an informative parameter of a proper analog input signal are considered. Relative error of formation of a dwell (lag) is calculated as a ratio of an absolute error (difference between an actual and a specified value) to a specified dwell (lag) value. As an actual value a result of a direct estimation of a dwell (lag) is accepted using measurement facilities.

Limits of allowed absolute errors of output (withdrawal) of commands and output signals and relative errors of formation of dwells and lags during a change of any EIF in a range of regulated for its limiting values are determined on agreement between the developer and the operating organization or the customer. For confirmation of compliance of alarm and control channels with specified requirements, checks of characteristic accuracy during a trial operation and periodic control during a preventive and predictive maintenance are provided.

Timing Performances

Timing performance is determined for each of the main functions of the I&C system and SHC in a form of nominal or maximal permissible (upper and / or low) values:

- Cycle time of data input from sensors and other I&C systems (SHC).
- Time resolution during data input and archiving.
- Lag of performance of discrete function.
- Speed of function execution.
- Rate of exchange through communication lines and local networks.
- Time of information storage in a data base and an archive.
- Time of start actuation after power restoration.

Nominal value of time resolution during data input and archiving are determined for accurate differentiation and registration of a sequence of initiating events, changes of state of technological equipment and controlled parameters, actions of control systems and personnel in an archive (for further analysis and estimation):

- For information of initiating events, violations of design limits of safety operation, occurrence of conditions of initiation of safety control systems, commands of protective actions – not worse than 0,01 sec.
- For information of a state of technological equipment, values of monitored parameters and set-points, violations of operational limits and conditions, commands of limitation, regulation, technological protection and interlocking, discrete and remote control - not worse than 0,1 sec.

Lags of performance of discrete functions (maximal permissible upper values):

- Output of Protection Commands: Not more than 0,1 sec, commands of limitation and interlocking - not more than 0,1 sec from a moment of an occurrence of a design specific condition till an occurrence of a control signal at the input of an actuating system or an element of technological equipment (except those commands, which should be generated with a specified lag).
- Execution of Remote Control Commands: Not more than 0,1 sec from the moment of signal generation at the output of a manual control key before occurrence of a control signal at the input of a proper actuating element of technological equipment.
- Warning of personnel and display of data about dangerous initiating events, violations of design limits and conditions, changes of monitored parameters and state of technological equipment, actuation of safety control systems and normal operation systems – not more than 1,0 sec from the moment of occurrence (change) till actuation of preventive or emergency alarm at workplaces of personnel and occurrence of a relevant information in the specified format of a data display device.
- Notification of personnel about operability failures, which affect safety, - not more than 10 sec (other - not more than 1 min) from failure occurrence till actuation of preventive alarm at workplaces.
- Archiving of data about initiating events, violations of design limits of safety operation, occurrence of conditions of generation protective action commands - 0,01 sec, data of a state of technological equipment, values of monitored parameters and set-points, violations of operational limits and conditions, commands of restriction, regulation, technological protection and interlocking, discrete and remote control - 0,1 sec between a time point of event occurrence and a time point at which it would be registered in a data base and an archive.
- Sampling on an operator call and display of information from a data base or an ar-

chive – not more than 2 sec from completion of directive input before occurrence of proper information in a specified format on a display device.

Function execution speed (maximal permissible number of functions, executed within a time unit):

- Calculation of design parameters for protection functions – not less than 100 times per second for each of parameters.
- Calculation of design parameters for functions of restriction, regulation, interlocking – not less than 10 times per second for each of parameters.
- Comparison of values of controlled parameters with set-points of preventive and emergency alarm – not less than 10 times per second for each of parameters.
- Archiving of data about initiating events, failures of design limits of safety operation, occurrence of conditions of generation protective action commands – not less than 100 times per second, data of a state of technological equipment, values of controlled parameters and set-points, violations of operational limits and conditions, commands of restriction, regulation, technological protection and interlocking, discrete and remote control – not less than 10 values per second for each of type of achieved data.
- Updating of video frame variable data, displayed in a monitor screen – not less than once per second.

Time of information storage in a data base (in operational memory of SHC) – not less than 24 hours, in an archive is usually within one fuel campaign of the reactor facility.

Time actuation start of a peripheral equipment and SHC after a short-term (not more than 10 min) of an intentional or unintentional disconnection and further power restoration of is determined in the form of a maximal permissible upper value, after its expiration an automatic recovery of execution of specified functions, interrupted due to power cut, is guaranteed. Execution of category A functions in a full scope with standardized properties is automatically resumed not later than in 1 min after power restoration, execution of category B and C functions – not later than in 5 min (or a bigger time interval – on agreement between a designer of the I&C system, the developer of SHC and the operating organization or a customer).

Human-Machine Interface

The I&C system and SHC, directly interacting with a personnel of NPP, should support the human-machine interface, whose properties allow minimizing personnel load and decreasing the probability of human errors. From the I&C system and SHC, human-machine interface is supported for:

- Alarm facilities (visual and audible alarm), multi-access information display (video monitors, informational screens and mimic panels), command input elements and operator’s guidelines placed in MCR, ECR and local control panels.
- Automated workplaces of operational personnel and/or workstations, placed in MCR and ECR.
- Workstations of operational personnel, placed in rooms of a shift engineer and/or technical support center.
- Automated workplaces of personnel, managing accidents, and safety experts, situated in emergency response centers.
- Elements of alarm, indication, display (video monitors, panel computers) and manual control elements, inbuilt into devices.

Human-machine interface facilities, placed in MCR and ECR, are labeled and placed in such a way that operational personnel could easily and accurately assess state of power unit and its systems, promptly detecting changes of state and executing provided actions required for power unit control. Workplaces of operational personnel in MCR and ECR meet ergonomics requirements, consider stereotypes of operators' behavior and human engineering. During design of workplaces mode of behavior of operational personnel in emergencies, when required actions should be simple, clear for understanding and execution, performed within a short time period and have not very long duration, are considered. Data display facilities and input elements of commands and guidelines are structured and identified taking into account their functions and priorities and their location corresponds to a logical sequence of actions of operational personnel during power unit control. It is provided that data display facilities placed in MCR and ECR and contained in post-accident monitoring systems visually differ from other display facilities, which are placed in the same rooms.

Information is displayed in video screens in the form convenient for perception and analysis, approved in practice and received a good grade from personnel. Each operator by its choice is provided with a generalized and / or detail information in the form of mimic planes, histograms, graphs, tables, logic diagrams, text messages, etc. Data about current values of controlled parameters, state of structures, systems and elements, output signals and commands, operability failures are automatically updated in a screen. Symbolic representation of sensors and actuators allow personnel to easily identify and accurately define their state (position) and operability. Information, displayed in video screens, is organized in a form of a system of independent fragments (still images) with an hierarchical structure that provides a possibility of a general view of a state of a controlled object and its sequential specification on several disaggregation levels ("general– to– specific"). Selection of still frames for display is carried out in simple and visual ways with a minimum number of required for it actions. Protection from the loss of important information due to overlaying and overlapping of still images during their actuation and / or in cases of change of sizes and location of screens by operator, in which still images are displayed, is provided.

Alarm messages, generated to workplaces of the operational personnel in case of detection of failures of design limits and/or normal and safety operation conditions, protection actuation, operability failure of a controlled object and in other specified cases, are displayed on video monitors in a dedicated screen area, not overlapped by other images. Text of the alarm message allows personnel to promptly and definitely detect a place, time, nature and if possible a degree of failure hazard. Output of alarm messages are followed by visual and / or audio signals, which have differences that allow personnel to qualitatively assess a degree of failure hazard. Facilities for shutdown of audio signals to avoid unnecessary acoustic load and attract attention to new alarm messages are provided. Visual alarm is activated till reasons, which caused the output of the alarm signal, will be eliminated, after that it is automatically stopped. Time period of occurrence and shutdown of alarm and a reason that caused the output of the alarm message, are registered in a data base.

The operator has a possibility to support reception of each identified alarm message, an authorization to prohibit the output of individual alarm messages and cancel prohibitions from his workplace. Confirmation of the reception of the alarm signal is displayed in the screen (for example, a change of color or conversion from blinking to a smooth glow) and causes the shutdown of the audio signal. Alarm message, whose reception was confirmed, is automatically deleted from the screen in case of elimination of failure that has caused it. Prohibition of the output of the alarm message is followed by its removal from the screen and shutdown of the audio signal. By operator's call a chronological list of all eliminated and remained failures, time period of its occurrence and elimination is shown in the screen.

Facilities of human-machine interface on workplaces of personnel, that controls a state and provides maintenance and recovery of the I&C system, are manufactured, labeled and placed in such a way that it would be possible to accurately assess a state of the system and its components, detect places of occurrence and a nature of operability failures and make a solution for their elimination.

INDEPENDENCE OF FUNCTIONS

Property of Independence

A group of mutually redundant I&C systems or SHC of 2(A) safety class remains operable and keeps specified properties during performance of category A functions independently from possible (considered by the project) external influencing factors and / or in case of deactivation, operability failure of one of these systems or SHC, and as a result of faulty actions of the personnel during their maintenance or recovery. A group of redundant channels of one I&C system or SHC of 2(A) safety class has similar properties. Each I&C system (SHC) of 2(A) safety class remains operable and keeps specified properties during performance of category A functions independently from the state of any element, a group of elements or a channel of the same system, intended for performance of lower category functions, or any adjacent I&C system (SHC) of lower safety class.

Independence from External Influencing Factors: (Such as fire, flood, extreme temperature and humidity, electromagnetic disturbances, etc.) and from faulty actions of personnel that provides maintenance or recovery, is provided by physical separation of components of different I&C systems, SHC and their redundant channels, and related cables (for examples, location of SHC in different rooms, using redundant channels of one SHC in separate cases or supporting constructions inside one case). Preferable ways of physical separation of cables are the use of individual cables of channels and penetrations.

Independence from Deactivation or Operability Violations: Of individual components of the I&C system, SHC or redundant channels is provided due to a functional and / or electric separation. Functional separation ("functional isolation") is provided by the fact that each I&C system (SHC, redundant channel) has a full set of input data required for performance of specified functions, electric separation - galvanic isolation and circuit shielding (electric separation is provided in cases, when for different I&C systems, SHC and / or redundant channels a common source of input data, a common signal receiver and / or one and the same power source are used).

For galvanic isolation electric, optic and other separation devices ("isolators"), fiber optic lines and local networks, transmitting information in the form of optic signals, are used. Quality of galvanic separation is defined by electric strength of isolation between galvanic isolated or isolating during the operation by electric circuits and between the enclosure and all isolated from the enclosure electric circuits of device and by resistance of electric isolation between the same circuits.

Electric strength of isolation is defined by the value of test voltage of a direct current or an amplitude value of the test voltage of an alternating current, being applied during one minute between a tested circuit and interconnected clips of other circuits, including safety-ground clips that do not cause breakdown or isolation breaking. Value of test voltage, depending on a device safety class, circuit nominal voltage and conditions for execution of tests, should be not lower than the specified ones in Table 16.

Electric isolation resistance between the tested circuit and interconnected clips of other circuits, including ground clips:

Table 16. Electric strength of isolation (test voltage)

Safety Class	Test Conditions (Temperature and Humidity)	Test Voltage for the Circuit with a Nominal Voltage		
		To 20 V Inclusive	Over 20 to 100 V Inclusive	Over 100 to 1000 V Inclusive
2(A)	upper working	1500 V	1500 V	2000 V
	upper limit	500 V	500 V	1200 V
3(B)	upper working	100 V	500 V	2000 V
	upper limit	60 V	300 V	900 V
3(C)	upper working	100 V	500 V	2000 V
	upper limit	60 V	300 V	900 V

- Not less than 40 MOhm under normal test conditions.
- Not less than 10 MOhm under an upper temperature working value.
- Not less than 2 MOhm under upper humidity working value.

Normal test conditions– naturally set in a room, where tests are executed, upper working values of a temperature and humidity– according to Table 2, upper limiting values – according to Table 3 and 4.

Independence from adjacent I&C systems, SHC and redundant channels are provided by:

- A selection of a structure of connections, interfaces and communication protocols through communication lines or a local network, which allow checking accuracy of obtained data and in case of failures of any of devices, connected to a local network, - to keep a possibility of communication between other devices.
- Use of hardware and software for control of data flows, protocol processing, detection and correction of errors in order that any failures during transmission and reception of messages do not influence on performance of specified functions of the I&C system (SHC).
- Use of different data transfer paths between redundant channels.

Independence of I&C systems, SHC and redundant channels, related to 2(A) and 3(B) safety classes, is also provided regarding all specified for them category B functions. For category C functions independence requirements are specified in reasoned cases on agreement between the designer of the I&C system (developer of SHC) and operating organization or the customer.

Permissible Disturbance Emission

Operating stand-alone component parts of SHC and peripheral equipment during operation, connection and disconnection do not create switching or other disturbances, which could cause operation failures of other components of the I&C system, connected to the same primary power network or to the same power source.

Level of radiated disturbances during operation, connection and disconnection of operating stand-alone component parts of SHC and peripheral equipment does not exceed values specified in CISPR, 2006 and an identical state standard of Ukraine that regulates requirements for informational technology equipment, intended for operation in manufacturing facilities.

For devices with a consumption current not more than 16 A (in a single phase), connected to a common primary power network, disturbance emission standards are specified (harmonic components of consumed current and/or voltage oscillations, caused by this current) in the primary power network.

Fire Safety

Operating stand-alone component parts of SHC and peripheral equipment meet requirements of fire-prevention standard of NAPB, 2000. Fire safety is provided under maximal permissible long- and short-term increase of power supply voltage, high voltage on inputs and outputs, short circuits inside a devices and output circuits. Fire prevention is provided:

- Use of fire-proof materials, coatings and cables (noncombustible, hardly inflammable, flame-retardant and nonsmoking and without toxic discharges) that passed specific tests and were certified according to the established procedure.
- Use of component parts, in which ignition sources do not occur during reloading, short circuits or failures.
- Voltage limitations, which can occur in input or output circuits in case of adjacent equipment failures or as a result of personnel errors.
- Use of active facilities of control, or protective shutdown of ignition sources, or automatic device de-energizing in case of detection of fire hazards.

Probability of fire in any operating stand-alone device is not more than10^{-6} a year. For prompt ignition detection inside a device, a continuous automatic monitoring and a preventive alarm in case of detection of hazards (temperature increase, smoke in a case) are provided. For operating stand-alone devices related to 2(A) safety class, requirements for monitoring and alarm in case of ignition detection in a device are mandatory, for devices of other safety classes – recommended.

For prompt fire detection and making solutions for its elimination, informational systems of fire alarm and / or control systems of automatic firefighting, related to 2(A) safety class, should be provided. Fire alarm and automatic firefighting systems (Bachmatch, 2008) are developed, designed and placed in such a way to guarantee that their spurious actuation will not affect other systems.

SOFTWARE PROPERTIES

For software of the I&C system, SHC and intellectual peripheral equipment requirement are regulated: for functions, structure and elements; for diagnostics and self-control; for protection against failures, corruptions, unforeseen actions. Similar requirements are provided for electronic design of complex programmable components.

Functions, Structure and Elements: Software provides performance of all functions, that should be executed or using with a specified reliability and quality of operation. Software of the I&C system, SHC and peripheral equipment has a module structure. Text of one module contains a limited number of operators, has a clear structure, can be easily modified and tested.

The software that is used as a component in the I&C system, SHC and peripheral equipment of 2(A) safety class, the use of operating systems is limited by only the simplest functions. In software that is used as a component of the I&C system, SHC and peripheral equipment of 3(B) safety class, the use of interruptions is limited, in case of performance of category A functions – is prohibited. In software, participating in execution of category B and C functions, operating system and interruptions are used only in reasoned cases.

Diagnostics and Self-Control: Software performs a continuous automatic monitoring of a technical state of the I&C system, SHC or peripheral equipment and provides technical diagnostics with a regulated integrity, depth, reliability, efficiency and periodicity.

Software performs diagnostics of its software ("self-control"), for example, using methods of a repeat count and comparison of results, detection of prohibited situations, assessment of duration of execution of programs, procedures, etc. Software provides automatic registration, storage and display of data of results of diagnostics and self-control. Recoding of programs of self-control diagnostics do not influence execution of main functions of software and does not cause degradation of their properties. Failures (errors during execution) of diagnostic and self-control programs do not affect execution of main functions of the I&C system, SHC or peripheral equipment.

Service software provides automation of periodic monitoring of the I&C system, SHC and peripheral equipment during maintenance and periodic checks (testing).

Protection Against Failures, Corruptions, Unforeseen Actions: Based on results of technical diagnostics and provides reconfiguration of structures of the I&C system (SHC) and computation process recovery. Software executes automatic checking of input information, warning of personnel in case of unreliability detection and protection from hazardous effects, which could be caused by data corruption. In software protection against computer viruses is [provided. As general methods of protection, for example, the following are applied:

- Control of integrity of system areas, launched application programs and used data.
- Control of events, critical for a safety system.
- Prevention of a negative result in case of a random launch of actions not specified by specifications.
- Creation of a safety and isolated operational environment.
- Detection of informational files in a purchased software, a read-only memory of purchased component parts and complex electronic components.
- Software safety recovery.

Detailed information on software in safety important NPP I&C systems is described in Chapter 5.

Solutions and Recommendations

The compliance of discussed in this chapter the properties of I&C systems and their components (software-hardware complexes and peripheral equipment) to the requirements of national and international regulations, rules and standards is a necessary, but not sufficient condition for functional safety these systems assessment. To ensure the functional safety it have to be complemented the second condition – the fulfillment of order of I&C systems design, manufacturing, testing, inspection and maintenance, as well as the same to hardware- software complexes and peripheral equipment for these systems. This condition is mentioned, but wasn't detailed in this chapter and requires the separate consideration.

Particularly, recommend to include the requirements to these processes at all stages of the life cycle of I&C systems and their components to new Ukrainian regulations on I&C functional safety.

FUTURE RESEARCH DIRECTIONS

Directions of work on further improvement of properties of safety important I&C systems and their components:

1. Extension of a set of requirements for properties of I&C systems and their components, which should be regulated by norms, rules and standards of nuclear and radiation safety

and controlled during the process of design, development, manufacturing, implementation and/or commissioning:

   a. Concerning cyber security of safety I&C systems.
   b. Concerning resistance and immunity of a peripheral equipment to external influencing factors possible in conditions of design basis and beyond design basis accidents.

2. Provision in the following standards and regulatory documents, taking into account native and international experience:
   a. Rules for design of safety important I&C systems, development of software-hardware complexes, peripheral equipment and software for these systems, qualification of commercial-off-the-shelf products and programs.
   b. Methods for determination of properties of I&C systems and their components at all life cycle stages, assessment criteria and rules for confirmation of compliance with specified requirements.
3. Assessment of the possibility to continue operation of I&C systems and their components after expiration of the period specified by manufactures:
   a. Regulatory and methodological support of work, including specification of qualification requirements.
   b. Qualification tests of operational I&C systems, software-hardware complexes and peripheral equipment (sensors, actuators).
   c. Assessment of results of qualification testing and decisions of continuation of operation of I&C systems and their components, whose properties correspond to specified qualification requirements.
4. Modernization of earlier developed (operational) I&C systems, including replacement of software-hardware complexes and peripheral equipment, which did not pass qualification testing, operated the with a significant exceeding of regulated period and / or may being a reason of unit operation failures.
5. Improvement and adaptation of national normative base of Ukraine, including implementation of requirements of new international safety standards (IAEA, 2011,a; IAEA 2012; IEC 2011, etc.):
   a. Revision and development of new national regulations.
   b. Development of standards establishing detail technical requirements for I&C systems and their components, as a result of these regulations.

CONCLUSION

Properties of safety important I&C systems and their components are determined by the requirements in the regulations, rules and standards of nuclear and radiation safety, acted in Ukraine, safety standards of IAEA and IEC,, international industrial standards of IEC, International Special Committee on Radio Interference, etc., as well as state standards of Ukraine, identical with relevant international standards.

In Chapter 3 are described properties of safety important I&C systems and their components:

- Functional properties of I&C systems.
- Reliability of I&C functions execution (coping with common cause failures, observance of single failure criterion, redundancy, diversity principle, prevention of personnel errors, protection from unauthorized access, technical diagnostic).

- Resistance of functions execution (stability to the environment, mechanical, seismic influences, immunity to electrical action, change of power parameters, electromagnetic disturbances), what are described more detailed.
- Quality of functions execution (accuracy, timing performances, human-machine interface).
- Independence of functions execution, include permissible disturbance emission and fire safety.

Properties of I&C systems have differences for various countries and are changing in time. Information in Chapter 3 defines "country- time profile" and can be used for comparison of I&C systems properties, what are used in different countries or are elaborated now.

REFERENCES

Anikanov, S., Bezsalyj, V., et al. (2003). Maintenance and safety assessment of nuclear power plant safety parameters display systems of WWER-1000 reactor. *Nuclear and Radiation Safety, 1*.

Bachmatch, E., Marshevsky, M., Rozen, Y., et al. (2008). Assurance and safety assessment of fire-alarm systems and automatic fire extinguishing in the accommodations NPP. *Nuclear and Radiation Safety, 3*.

Bachmatch, E., Vinogradska, S., Rozen, Y., et al. (2005). The software-hardware complexes for the power automatic regulation, reactors power reduction and limitation and acceleration preventive protection: the safety insurance and assessment. *Nuclear and Radiation Safety, 1*.

Belohin, O., et al. (2010). Automatic control system of diesel-generator for NPP: Emergency supply. Westron. Retrieved from http://www.westron.kharkov.ua/SAU_RDES.pdf

CISPR. (2006). CISPR 22 . *Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement*.

Gorelik, A., Eliseev, V., Kugil, A., et al. (2005). Conception of in-core reactor monitoring system modernization of Uktainian NPP. *Nuclear and Radiation Safety, 2*.

IAEA. (2000). NS-G-1.1. *Software for computer based systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2002a). NS-G-1.3. *Instrumentation and control systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2002b). NS-G-2.3. *Modifications to nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2011a). SSR-2/2. *Safety of nuclear power plants: Commissioning and operation: Specific safety requirements*. Vienna, Austria: IAEA.

IAEA. (2011b). NP-T-3.12. *Core knowledge on instrumentation and control systems in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (2012). SSR-2/1. *Safety of nuclear power plants: Design: Specific safety requirements*. Vienna, Austria: IAEA.

IEC. (1996). IEC 60980. *Recommended practice for seismic qualification of electrical equipment for nuclear power generating stations.*

IEC. (1998). IEC 60780. *Nuclear power plants - Electrical equipment of the safety system – Qualification*.

IEC. (2001a). IEC 61000-4-2. *Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test.*

IEC. (2001b). IEC 61000-4-3. *Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity.*

IEC. (2001c).: IEC 61000-4-4. *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques - Electrical fast transient / burst immunity test: Basic EMS publication.*

IEC. (2001d). IEC 61000-4-8. *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test.*

IEC. (2001e). IEC 61000-4-9. *Electromagnetic compatibility (EMC) – Part 4-9: Testing and measurement techniques - Pulse magnetic field immunity test.*

IEC. (2001f). IEC 61000-4-10. *Electromagnetic compatibility (EMC) – Part 4-10: Testing and measurement techniques - Damped oscillatory magnetic field immunity.*

IEC. (2001g). IEC 61000-4-12: *Electromagnetic compatibility (EMC) – Part 4-12: Testing and measurement techniques - Oscillatory waves immunity test.*

IEC. (2002a). IEC 61000-4-14: *Electromagnetic compatibility (EMC) – Part 4-14: Testing and measurement techniques - Voltage fluctuation immunity test.* IEC.

IEC. (2002b). IEC 61000-4-16. *Electromagnetic compatibility (EMC) – Part 4-16: Testing and measurement techniques - Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz.*

IEC. (2002c). IEC 61000-4-28. *Electromagnetic compatibility (EMC) – Part 4-28: Testing and measurement techniques - Variation of power frequency, immunity test.*

IEC. (2004). IEC 61000-4-11. *Electromagnetic compatibility (EMC) – Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests.*

IEC (2005a). IEC 62138. *Nuclear power plants - Instrumentation and control important for safety -. Software aspects for computer-based systems performing category B or C functions.*

IEC. (2005b). IEC 61000-4-5. *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques - Surge immunity test.*

IEC. (2006a). IEC 61000-4-6. *Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields.*

IEC. (2006b). IEC 60880. *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.*

IEC. (2007a). IEC 60987. *Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems.*

IEC. (2007b). IEC 62340. *Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF).*

IEC. (2008). IEC 61508. *Functional safety of electrical/electronic/programmable electronic safety related systems.*

IEC. (2009). IEC 61226. *Nuclear power plants -Instrumentation and control systems important to safety – Classification.*

IEC. (2011). IEC 61513. *Nuclear power plants - Instrumentation and control important to safety - General requirements for systems.*

ISO. (2000). ISO 9001. *Quality management systems – Requirements.*

NAPB. (2002). NAPB 03.005. *Fire protection: Firefighting norms development of nuclear power plants with pressured water reactors.* Kiev, Ukraine: Ministry of Fuel and Energy.

NP. (1999). NP 306.5.02/3.017. *Quality assurance program requirements at all stages life-cycle of the nuclear power plant.* Kiev, Ukraine: State Committee for nuclear regulation.

NP. (2000). NP 306.5.02/3.035. *Requirements for nuclear and radiation safety information and control systems important to safety of nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2003a). NP 306.5.02/2.068. *Requirements for the order and scope of work to extend the term operation activity of information and control systems, important to safety of nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2003b). NP 306.5.02/3.076. *Requirements for the organization and order of commissioning power plant*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2005). NP 306.2.106. *Requirements for the modification of the nuclear installations and their safety evaluation order*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2008a). NP 306.2.141. *General provisions on the safety of nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2008b). NP 306.2.145. *Nuclear safety regulations the reactors nuclear power plants with pressurized water reactors*. Kiev, Ukraine: State Committee for Nuclear Regulation.

PNAE. (1987). PNAE G-5-006. *Rules of design earthquake-resistant nuclear power plants*. Moscow: Gosatomenergonadzor.

Rozen, Y. (2007). Electromagnetic compatibility of instrumentation and control systems components (1), rules for regulations and estimation. *Nuclear and Radiation Safety, 2*.

Rozen, Y. (2008). Electromagnetic compatibility of instrumentation and control systems components (2), Устойчивость к электромагнитным помехам. *Nuclear and Radiation Safety, 4.*

ADDITIONAL READING

Biscoglio, I., & Fusani, M. (2010). Analyzing quality aspects in safety-related standards. *Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010*, Las Vegas, Nevada, American Nuclear Society

Hashemian, H. (2006). *Maintenance of Process Instrumentation in Nuclear Power Plants*. Berlin, Heidelberg, New York: Springen.

IAEA NP-T-1. 4 (2008). *Implementing digital instrumentation and control systems in the modernization of nuclear power plants,* Vienna, Austria: IAEA.

IAEA NP-T-1. 5 (2009). *Protecting Against Common Cause Failures in Digital I&C Systems,* Vienna, Austria: IAEA...

IAEA-TECDOC-1016 (1998). *Modernization of Instrumentation and Control in Nuclear Power Plants*, Vienna, Austria: IAEA.

IEEE 1289 (1998). IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations.

IEEE Std 379 (2000). Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.

IEEE Std 323 (2003). Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 323 (2003). Qualifying Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 344 (2004). Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 344 (2004). Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 384 (2008). Standard Criteria for Independence of Class 1E Equipment and Circuits.

IEEE Std 627 (2010). IEEE Standard for Qualification of Equipment Used in Nuclear Facilities.

Yastrebenetsky, M., Rozen, Y., Klevtsov, A., et al. (2012) *Fukushima accident lessons for I&C systems (Ukrainian experience, first steps).* 8 th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies (NPIC & HMIT), San Diego, USA.

KEY TERMS AND DEFINITIONS

Common Cause Failures: A simultaneous failure of two or more elements in different redundant parts due to the same cause, which can result in a failure of I&C function.

Diversity: A property related to a group of two or more I&C systems and SHC, which simultaneously and independently from each other perform functions identical for achieved safety purposes, and differ from each other by the operating principle, structure, applied component parts, software and / or other attributes or achieve the target goal in different ways.

External Influencing Factors (EIF): Factors, which can occur in places of hardware r location and include: EIF environment (temperature, humidity, barometric pressure, ionizing radiation, corrosive agents, dust), mechanical EIF (vibrations, strokes, seismic effects), EIF power supply, EIF spe cific environments (water and solutions, which can affect devices in accidents and to decontamination fluids), . electromagnetic EIF.

Redundancy: Application of additional means and / or possibilities, redundant in regard to those, that are minimally required for function performance.

Single Failure Criterion of I&C Systems and SHC: Criterion which requires performing all specified functions in any postulated initiating event (PIE), with combination of failure of one (any) element independent of this PIE.

Chapter 4

Field Programmable Gate Array Technology for NPP I&Cs

Vladimir Sklyar
Research and Production Corporation Radiy, Ukraine

Anton Andrashov
Research and Production Corporation Radiy, Ukraine

Eugene Babeshko
National Aerospace University named after N.E. Zhukovsky KhAI, Ukraine

Andriy Kovalenko
Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

ABSTRACT

FPGA is a convenient technology that is being applied intensively to build I&CS for critical industries like NPPs. Practical experience confirms that in some cases application of the FPGA technology is much more reasonable than application of other technologies like microprocessors, etc. Experience of RPC Radiy in FPGA-based I&C development is provided in this chapter, as well as general information on FPGAs. Dependability of NPP I&CS is an important but challenging task. There are several techniques that can be applied for safety and dependability assessments, but all of them have limitations and cannot be easily applied in most cases. Sometimes combined usage of different methods is the most appropriate solution. Techniques of dependability assessment and achievement developed and used by RPC Radiy, as well as elements of the assessment methodology are briefly described.

INTRODUCTION

Nuclear power production is a safety-critical process that requires reliable and safe operation. Information & control systems (I&Cs) of nuclear power plants (NPP) play key roles in stable operation ensuring and therefore should be designed in accordance with international requirements on nuclear and operational safety.

One of the contemporary trends is dynamically growing application of novel complex electronic components, particularly, FPGAs in NPP I&Cs and other critical areas. I&C systems based on Field programmable gate array (FPGA) technology

DOI: 10.4018/978-1-4666-5133-3.ch004

have been developed and applied in aerospace and process industries since the 1990s. Although the use of FPGAs in NPPs I&C systems has lagged behind in the past compared to other industries, there is an increasing number of FPGA installations in operating NPPs.

BACKGROUND

The FPGA technology offers an alternative to microprocessor (or computer) technologies and to other types of programmable logic devices. Physically, FPGA is a semiconductor-based complex programmable device which can be configured to perform a required function.

It includes two entities: an FPGA chip, which is a piece of hardware that can be qualified against hardware qualification testing requirements, and the electronic design of the FPGA, implemented into a chip, represented by a set of instructions in hardware description language (HDL) that can be verified against functional requirements.

Problem is development of new approach to assessment of FPGA-based systems for NPP I&Cs taking into account of the FPGA technology features.

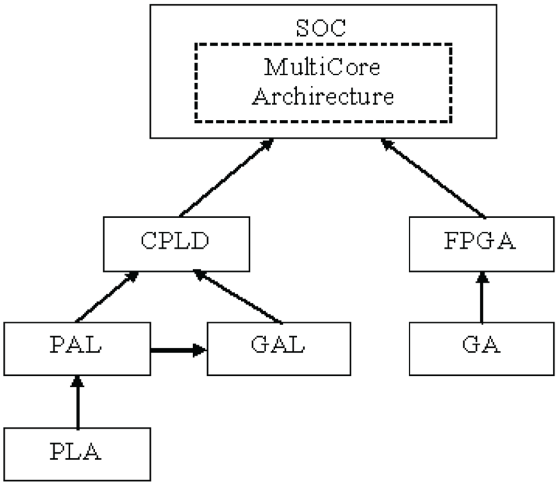
FEATURES OF FPGA TECHNOLOGY AND THEIR APPLICATION IN NPP I&CS

This subsection provides results of comprehensive analysis of FPGA technology features, including approaches to implementation of FPGA-based development activities, as well as possible applications of the technology.

Features of FPGA Technology

There are two lines in contemporary programmable logic arrays (Kharchenko, V. S., Sklyar, V. V. (Ed.), 2008; Barkalov, A., Wegrzyn, M. et al., 2006): Complex Programmable Logic Devices (CPLD) and Field Programmable Gates Arrays (FPGA). CPLDs are a continuation of programmable matrix logic line, whereas FPGAs continue basic matrix crystal line. The desire to combine the advantages of both line led to development of combined architecture VLSIs (see Figure 1). Still, all contemporary FPGAs possess such architecture. We shall discuss FPGAs of APEX II family produced by Altera as representatives of combined architecture.

Figure 1. Architecture types of FPGA



CPLD architecture has its origins in Programmable Arrays Logic (PAL) preceded by Programmable Logic Arrays (PLA) and from Generic Arrays Logic (GAL). Its functional unit consists of microcells, each of them performing some combinatory and/or register functions. Functional logic within the block is a matrix of logic products (terms). A subset of terms may be accessed by each macrocell via term distribution diagram. Switch matrix commutates the signals coming from outputs of the functional unit and I/O unit. As distinct from FPGA (segmented connections), CPLDs have a continuous system of connections (completely commuted connections).

FPGA architecture topologically originates from channeled Gates Arrays (GA). In FPGA internal area a set of configurable logic units is disposed in a regular order with routing channels there between and I/O units at the periphery. Transistor couples, logic gates NAND, NOR (Simple Logic Cell), multiplexer-based logic modules, logic modules based on programmable Look-Up Tables (LUT) are used as configurable logic blocks. All those have segmented architecture of internal connections.

System-On-Chip (SOC) architecture appeared due to two factors: high level of integration permitting to arrange a very complicated circuit on a single crystal, and introduction of specialized hardcores into FPGA. Additional hardcores may be:

- Additional Random Access Memory (RAM) units.
- JTAG interface for testing and configuration.
- **Phase-Locked Loop (PLL):** Frequency control system to correct timing relations of clock pulses as well as for generation of additional frequencies.
- Processor cores enabling creation of devices with a control processor and a peripheral.

FPGA resources and additional RAM are disposed at the processor address space. The examples of such solutions are the families of Altera Excalibur (Embedded Processor Programmable Solution), Atmel FPSLIC AT94 (Field Programmable System Level Integration Chip).

Tables 1-4 specify the main characteristics of modern FPGA chips from Altera (for more information see altera.com).

Manufacturer guarantees pre-sale testing of 100% FPGAs.

Unlike projects based on Applications Specific Integrated Circuit (ASIC), which have a fixed architecture (fixed IC outlets, IC functionality cannot be altered), FPGAs are reconfigurable.

FPGAs (when the system is fed) are configured by data stored at the configuration device or by those supplied from the system controller. Altera CASE-tools enable programming of devices within the system. They configure FPGA with a consecutive flow of data.

Moreover, FPGAs comprises an optimized interface using microprocessors for serial or parallel, synchronous or asynchronous configuration of those devices. This interface also enables microprocessors to interpret FPGAs as memory and to configure them by recording to memory cell virtual address, thus facilitating the reconfiguration process.

FPGAs consist of several MegaLAB structures. Each MegaLAB comprises 16 LAB – Logic Arrays Blocks, one built-in systemic memory – Embedded System Block (ESB) and a MegaLAB connection which routes signals within the structure between MegaLAB structures and I/O leads via FastTrack connection. Besides, LAB signal fronts may be controlled via local connection using I/O leads.

Each LAB comprises ten Logic Elements (LE), auxiliary transfers of logic elements and stage circuits, LAB control signals and a local interconnection that transmits signals between LEs in the same or an adjacent LAB as well as to IOE or ESB cells.

Table 1. Characteristics of circuits of Arria 10 GX family (20nm technology)

		Maximum Resource Count for Arria 10 GX FPGAs				
		10AX016	**10AX022**	**10AX027**	**10AX032**	**10AX048**
Resources	ALMs	61,510	81,510	101,620	119,660	182,720
	LEs (K)	160	220	270	320	480
	Registers	246,040	326,040	406,480	478,640	730,880
	M20K memory blocks	440	583	750	891	1,438
	M20K memory (Mb)	9	11	15	17	28
	MLAB memory (Mb)	1	1.4	2.2	2.9	4.4
	Variable-precision digital signal processing (DSP) blocks	156	192	800	985	1,368
	18 x 19 multipliers	312	384	1,600	1,970	2,736
		10AX057	**10AX066**	**10AX090**	**10AX115**	
	ALMs	217,080	251,450	339,620	427,700	
	LEs (K)	570	660	900	1,150	
	Registers	868,320	1,005,800	1,358,480	1,710,800	
	M20K memory blocks	1,850	1,964	2,339	2,713	
	M20K memory (Mb)	36	39	46	54	
	MLAB memory (Mb)	5.0	5.7	9.2	12.7	
	Variable-precision digital signal processing (DSP) blocks	1,612	1,855	1,518	1,518	
	18 x 19 multipliers	3,223	3,356	3,036	3,036	
		10AX016	**10AX022**	**10AX027**	**10AX032**	**10AX048**
Architectural Features	Global clock networks	32				
	Regional clock networks	8	8	8	8	8
	Design security	Bitstream encryption with authentication				
		10AX057	**10AX066**	**10AX090**	**10AX115**	
	Global clock networks	32				
	Regional clock networks	8	16	16	16	
	Design security	Bitstream encryption with authentication				
		10AX016	**10AX022**	**10AX027**	**10AX032**	**10AX048**

continued on following page

CASE Quartus II compiler places the project-associated logic within LABs or LAB auxiliary blocks, thus permitting usage of quick-acting local interconnections to increase the capacity of system designed. APEX FPGAs use LAB intermittent structure in such a way that each LAB is able to control two areas of local interconnections.

Each LAB structure may control thirty LEs using quick-acting local interconnections. Figure 2 shows LAB structure for APEX II family FPGAs.

Each LE controls left or right area of local interconnections intermittent by LEs, whereas a local interconnection controls LEs within its own LAB or adjacent LABs. This property optimizes

Table 1. Continued

		Maximum Resource Count for Arria 10 GX FPGAs				
I/O Features	I/O voltage levels supported (V)	1.2, 1.25, 1.35, 1.8, 2.5, 3.0				
	I/O standards supported	3 V I/Os Only: 3 V LVTTL, 2.5 V CMOS DDR and LVDS I/Os: POD12, POD10, Differential POD12, Differential POD10, LVDS, RSDS, mini-LVDS, LVPECL All I/Os: 1.8 V CMOS, 1.5 V CMOS, 1.2 V CMOS, SSTL-18 (I and II), SSTL-15 (I and II), SSTL-135, SSTL-125, SSTL-12, HSTL-18 (I and II), HSTL-15 (I and II), HSTL-12 (I and II), HSUL-12, Differential SSTL-18 (I and II), Differential SSTL-15 (I and II), Differential SSTL-135, Differential SSTL-125, Differential SSTL-12, Differential HSTL-18 (I and II), Differential HSTL-15 (I and II), Differential HSTL-12 (I and II), Differential HSUL-12				
	LVDS channels, 1.6 Gbps (receive/transmit)	120	120	168	168	222
	Embedded dynamic phase alignment (DPA) circuitry	yes				
	On-chip termination (OCT)	Series, parallel, and differential				
	Transceiver count	12	12	24	24	36
	PCI Express® (PCIe®) hard IP blocks (Gen3)	1	1	2	2	2
	Memory devices supported	DDR4, DDR3, DDR2, QDR IV, QDR II+, QDR II+ Xtreme, LPDDR3, LPDDR2, RLDRAM 3, RLDRAM II, LLDRAM II, HMC				
		10AX057	**10AX066**	**10AX090**	**10AX115**	
	I/O voltage levels supported (V)	1.2, 1.25, 1.35, 1.8, 2.5, 3.0				
	I/O standards supported	3 V I/Os Only: 3 V LVTTL, 2.5 V CMOS DDR and LVDS I/Os: POD12, POD10, Differential POD12, Differential POD10, LVDS, RSDS, mini-LVDS, LVPECL All I/Os: 1.8 V CMOS, 1.5 V CMOS, 1.2 V CMOS, SSTL-18 (I and II), SSTL-15 (I and II), SSTL-135, SSTL-125, SSTL-12, HSTL-18 (I and II), HSTL-15 (I and II), HSTL-12 (I and II), HSUL-12, Differential SSTL-18 (I and II), Differential SSTL-15 (I and II), Differential SSTL-135, Differential SSTL-125, Differential SSTL-12, Differential HSTL-18 (I and II), Differential HSTL-15 (I and II), Differential HSTL-12 (I and II), Differential HSUL-12				
	LVDS channels, 1.6 Gbps (receive/transmit)	270	270	384	384	
	Embedded dynamic phase alignment (DPA) circuitry	yes				
	On-chip termination (OCT)	Series, parallel, and differential				
	Transceiver count	48	48	96	96	
	PCI Express® (PCIe®) hard IP blocks (Gen3)	2	2	4	4	
	Memory devices supported	DDR4, DDR3, DDR2, QDR IV, QDR II+, QDR II+ Xtreme, LPDDR3, LPDDR2, RLDRAM 3, RLDRAM II, LLDRAM II, HMC				

Table 2. Characteristics of circuits of Stratix V GS family (28nm technology)

		Maximum Resource Count for Stratix V GS FPGAs (0.85 V)				
		5SGSD3	**5SGSD4**	**5SGSD5**	**5SGSD6**	**5SGSD8**
Resources	ALMs	89,000	135,840	172,600	220,000	262,400
	LEs (K)	236	360	457	583	695
	Registers	356,000	543,360	690,400	880,000	1,049,600
	M20K memory blocks	688	957	2,014	2,320	2,567
	M20K memory (Mb)	13	19	39	45	50
	MLAB memory (Mb)	2.72	4.15	5.27	6.71	8.01
	Variable-precision digital signal processing (DSP) blocks	600	1,044	1,590	1,775	1,963
	18 x 18 multipliers	1,200	2,088	3,180	3,550	3,926
Architectural Features	Global clock networks	16				
	Regional clock networks	92				
	Design security	yes				
I/O Features	I/O voltage levels supported (V)	1.2, 1.5, 1.8, 2.5, 3.3				
	I/O standards supported	LVTTL, LVCMOS, PCI, PCI-X, LVDS, mini-LVDS, RSDS, LVPECL, Differential SSTL-15, Differential SSTL-18, Differential SSTL-2, Differential HSTL-12, Differential HSTL-5, Differential HSTL-18, SSTL-15 (I and II), SSTL-18 (I and II), SSTL-2 (I and II), 1.2 V HSTL (I and II), 1.5 V HSTL (I and II), 1.8 V HSTL (I and II)				
	LVDS channels, 1.4 Gbps (receive/transmit)	108	174	174	210	210
	Embedded dynamic phase alignment (DPA) circuitry	yes				
	On-chip termination (OCT)	Series, parallel, and differential				
	Transceiver count (14.1 Gbps)	24	36	36	48	48
	PCIe hard IP blocks (Gen3)	1	1	1	2	2
	Memory devices supported	DDR3, DDR2, DDR, QDR II, QDR II+, RLDRAM II, RLDRAM 3				

the number of available lines and columns of interconnections, thus ensuring their high flexibility.

Each LAB comprises a predestined logic to manage control signals to LEs and ESBs. Control signals may be timing, timing enable, asynchronous reset, pre-installation and loading, synchronous cleanup and synchronous boot. Maximum six signals may be passed simultaneously. Though synchronous boot and cleanup signals are mainly used for counter realization, they may perform other functions as well.

LE is the smallest part of logic in APEX II architecture. Each LE contains a LUT conversion table with four inputs that serves as a functional generator able of quick realization of any four-variables function. Besides, each LE includes a programmable register and transfer and staging circuits.

Each programmable register in LE may be configured to operate as a D, T, JK or SR trigger. Register timing and cleanup control signals may be accessed using global signals, general purpose I/O leads or any internal logic. To realize com-

Table 3. Characteristics of circuits of Stratix IV E family (40nm technology)

		Maximum Resource Count for Stratix IV E FPGAs (0.9 V)			
		EP4SE230	**EP4SE360**	**EP4SE530**	**EP4SE820**
Resources	ALMs	91,200	141,440	212,480	325,220
	LEs (K)	228	354	531	813
	Registers	182,400	282,880	424,960	650,440
	M9K memory blocks	1,235	1,248	1,280	1,610
	M144K memory blocks	22	48	64	60
	MLAB memory (Mb)	2,850	4,420	6,640	10,163
	Embedded memory (Kb)	14,283	18,144	20,736	23,130
	18 x 18 multipliers	1,288	1,040	1,024	960
Architectural Features	Global clock networks	16			
	Regional clock networks	64	88	88	88
	Periphery clock networks	88	88	112	132
	PLLs	4	12	12	12
	Design security	yes			
	Configuration file size (Mb)	95	141	172	230
	HardCopy series device support	yes			
	Others	Programmable Power Technology			
I/O Features	I/O voltage levels supported (V)	1.2, 1.5, 1.8, 2.5, 3.3			
	I/O standards supported	LVTTL, LVCMOS, PCI, PCI-X, LVDS, mini-LVDS, RSDS, LVPECL, Differential SSTL-15, Differential SSTL-18, Differential SSTL-2, Differential HSTL-12, Differential HSTL-15, Differential HSTL-18, SSTL-15 (I and II), SSTL-18 (I and II), SSTL-2 (I and II), 1.2 V HSTL (I and II), 1.5 V HSTL (I and II), 1.8 V HSTL (I and II)			
	Emulated LVDS channels, 1,100 Mbps	128	256	256	288
	LVDS channels, 1,600 Mbps (receive/transmit)	56/56	88/88	112/112	132/132
	Embedded dynamic phase alignment (DPA) circuitry	yes			
	On-chip termination (OCT)	Series, parallel, and differential			
	Memory devices supported	DDR3, DDR2, DDR, QDR II, QDR II+, RLDRAM 2, SDR			

binatory functions registers are omitted (routing performed without them), whereas LUT output controls LE output.

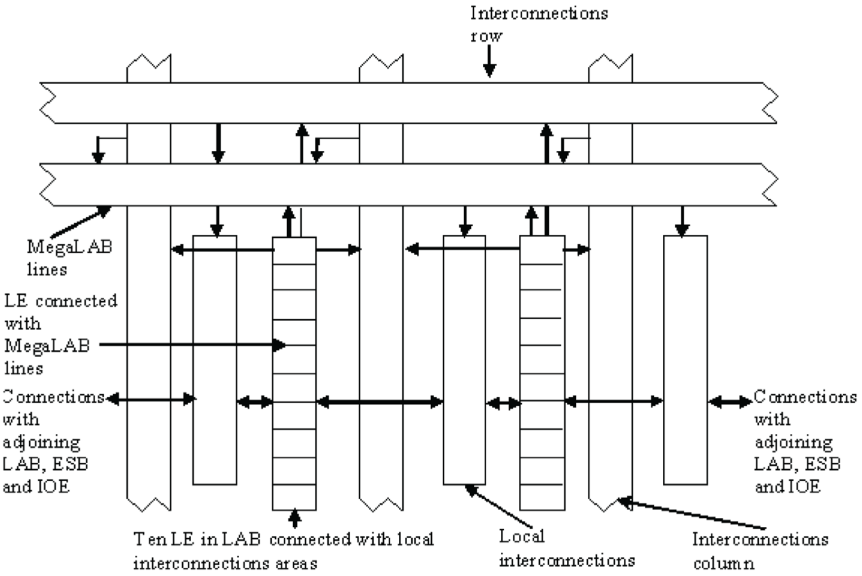
Each LE has two outputs that control such routing structures: local, MegaLAB or FastTrack interconnections. Each output may be operated irrespective from LUT or register output. For instance, LUT may operate one output, while register connects the other one. This property, called “register packing,” permits application of register and LUT to realize unconnected functions.

LE may also realize register and non-register options of LUT output.

Table 4. Characteristics of circuits of Cyclone III LS family (65nm technology)

		Maximum Resource Count for Cyclone III LS FPGAs (1.2 V)			
		EP3CLS70	**EP3CLS100**	**EP3CLS150**	**EP3CLS200**
Resources	LEs (K)	70	100	151	198
	M9K memory blocks	333	483	666	891
	Embedded memory (Kb)	2,997	4,347	5,994	8,019
	18 x 18 multipliers	200	276	320	396
Architectural Features	Global clock networks	20			
	PLLs	4			
	Configuration file size (Mb)	26.8	26.8	50.6	50.6
	Design security	yes			
	I/O voltage levels supported (V)	1.2, 1.5, 1.8, 2.5, 3.3			
	I/O standards supported	LVDS, LVPECL, Differential SSTL-18, Differential SSTL-2, Differential HSTL, SSTL-18 (I and II), SSTL-2 (I and II), 1.5 V HSTL (I and II), 1.8 V HSTL (I and II), PCI, PCI-X 1.0, LVTTL, LVCMOS			
	LVDS channels, 840 Mbps	169			
	On-chip termination (OCT)	Series and differential			
External Memory Interfaces	Memory device supported	DDR2, DDR, SDR			

Figure 2. LAB structure of circuits of APEX II family


Interconnections row
MegaLAB lines
LE connected with MegaLAB lines
Connections with adjoining LAB, ESB and IOE
Connections with adjoining LAB, ESB and IOE
Ten LE in LAB connected with local interconnections areas
Local interconnections
Interconnections column

FPGA Technology: Development Tools

During development activities, the use of proven tools is preferred over manual methods. Moreover, for development of safety critical I&C systems, software-based tools shall be purchased only from long-established vendors with a good track record of CM, V&V, problem notification and resolution, including help & training materials. Software tools should be selected and evaluated before their using in lifecycle processes.

One of the tools that can be used in development activities for FPGA-based NPP I&C systems is IDE Quartus II. It supports design and implementation stages, including VHDL coding, RTL synthesis, Netlist synthesis, Placement&Routing, Static timing analysis, and Bitstream generation. It also supports hardware and functional block libraries VHDL design entry, graphical-based design entry methods, and integrated system-level design tools. It integrates design, synthesis, place-and-route, and verification into a development environment.

IDE Quartus II from Altera has a wide range of capabilities such as design entry, simulation, synthesis, verification, and device programming. Generally IDE Quartus II as FPGA design software is widely used in different industries: military, medical equipment manufacturing, automotive electronic manufacturing, financial, bioscience, etc.

I&C system Design Entry is performed according to I&C system Requirements Specifications. The desired circuit is specified either by means of a schematic diagram, or by using a Hardware description language, such as VHDL or Verilog. Inputs documents for design stage typically are: Requirements Specifications, Electronic Design Architecture description, Electronic Design Detailed description. Results: VHDL files for HPDs.

Correctness of the design (Static Code Analysis) and its compliance with the requirements (Functional Testing) are verified after design phase. Software code verification is performed according to verification plan and testing plans which should be developed and approved before actions on software code verification.

Aldec Advanced Lint (ALINT™) tool can help to detect the design problems early in life cycle, including poor coding styles, improper clock and reset management, simulation, synthesis problems, poor testability and source code issues throughout the design flow. ALINT™ is a programmable design and coding guideline checker that speeds up development of complex system-on-chip designs. Certain rules may be parameterized to fine-tune custom checking policy. Policies combined with various ALINT settings allow development of unique rules checking framework for each design.

VHDL functional testing can be performed with ModelSim Altera tool, which uses either Verilog HDL or VHDL design files, including models for the library of parameterized modules and Altera megafunctions, to generate a functional simulation output of the design based on the set of stimulus applied by the user. Once the design is verified to be functionally correct, the next step is to perform implementation stage (synthesize the design and use the Quartus II software for place-and-route).

ModelSim-Altera software version is compatible with the specific Quartus II tool version. Proper verification of designs at the functional and post place-and-route stages using the ModelSim-Altera software helps ensure design functionality and, ultimately, a quick time-to-market.

Typically, implementation includes the following stages

- Synthesis (bringing in) of project scheme may be effected using schematic editor (library of elements), hardware description language or automaton state flow graph editor. Functional modules may be developed by various tools, but the data obtained are then united into a single circuit list.

- Translation of data from Electronic Design Interface Format (EDIF) Native Generic Database (NGD) internal format.
- Crystal mapping, i.e. transformation of designed logic elements to their physical counterparts.
- Placement of physical element and routing of their interconnections. On this stage ModelSim tool is used for Verification of Netlist Files & Floor Plan Files generated by Quartus II tool (Logic Simulation, Timing Simulation, Static Timing Analysis).

Application of ModelSim to automate verification environment allows significantly decrease time of verification.

Compliance of developed FPGA-based I&C system with the required functionality can be verified with a testbed, which simulate inputs and allows to test outputs and performance. National Instruments LabView is an automated test software that provides with the tools to create any testing, measurement and control systems. It simplifies system design by offering access to the newest high-performance and low-cost entry points to the reconfigurable I/O platform made by National Instruments Corp., to one of the highest bandwidth vector signal analyzers on digitizers on the market, and to the latest off-the-shelf hardware.

Let us discuss Atera Quartus II tool in details. Quartus II has such basic functional possibilities: usage of hardware description language, project scheme input, compilation, logic synthesis, full timing and functional simulation, analysis of worst timing case, logic analysis, device configuration (Kharchenko, V. S., Sklyar, V. V. (Ed.), 2008).

Quartus II includes LogicLock step design package, that permits laying destination of outputs and timing parameters, test functionalities and capacities of designed systems and then establish limitations in order to "lock" (fix) arrangement and characteristics of a specific logic block by applying LogicLock limitations.

The limitations as established by LogicLock functions ensure identical arrangement when logic block is performed within a current project or transferred to another project. LogicLock limitations may "lock" logic at a fixed position within the device. LogicLock may also specify a part of project logic for later optimization of its arrangement in an IC. Addition of logic to a project would not affect the properties of blocks "locked" LogicLock limitations.

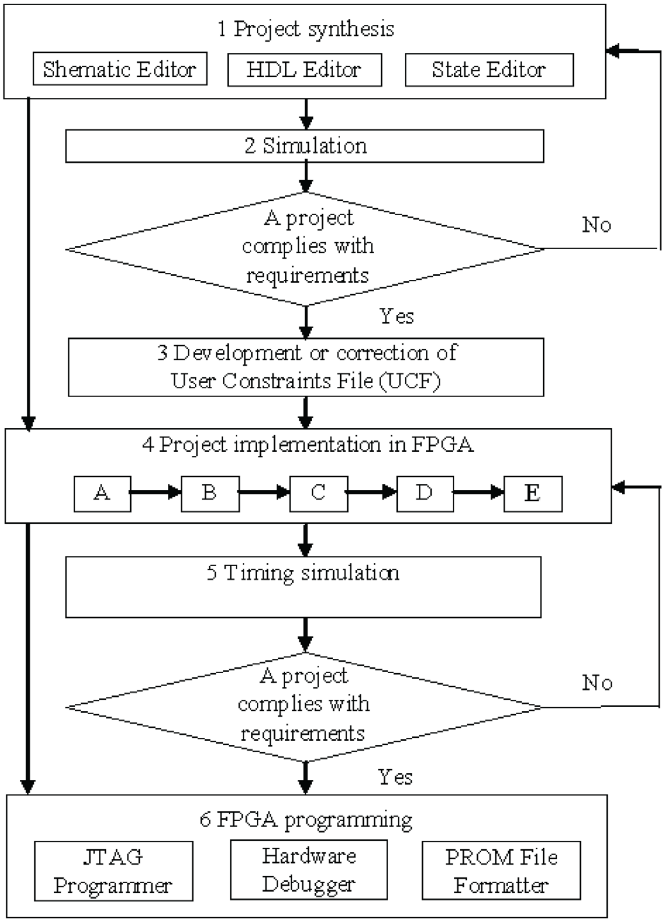
The process of design from project synthesis to its realization in a crystal is fully supported by CASE-tools (Melnyk, A. et al., 2007; Tam, S., 2003) (Figure 3). The following is a short description of six design process stages.

- Synthesis (bringing in) of project scheme may be effected using schematic editor (library of elements), hardware description language or automaton state flow graph editor.

Functional modules may be developed by various tools, but the data obtained are then united into a single circuit list.

1. Simulation is performed in order to test functioning of the project scheme with zero or single delays. Designer forms a diagram of input actions (test vectors).
2. Development or correction of User Constraint File implies description of requirements to arrangement of components and timing relations of signals using an appropriate editor.
3. Project implementation in FPGA includes:
    a. Translation of data from Electronic Design Interface Format (EDIF) Native Generic Database (NGD) internal format;
    b. Crystal mapping, i.e. transformation of designed logic elements to their physical counterparts;

Figure 3. Stages of tools-based FPGA-projects development



   c. Placement of physical element and routing of their interconnections;
   d. Timing of circuit delays and bit-stream generation.
4. Project is verified by simulation when actual timing values of delays as determined in the crystal are considered instead of zero or single values.
5. Crystal programming permits its JTAG, debugging and PROM file formatting for programmer.

Quartus II presents a large number of library functions for design, including buffers, triggers and latches, I/O registers and logic primitives. A feature of library functions is low integration level.

Besides, Quartus II presents plenty of architecturally optimized macrofunctions that reflect the specifics of FPGA application. The whole set of macrofunctions may be presented by such categories of typical schemes: adders, arithmetic logic devices, buffers, comparators, cipherers, counters, decoders, digital filters, error detectors and correctors, coding-decoding circuits, frequency dividers, latches, multipliers, multiplexors, registers, shift registers, low integration level elements, I/O gates.

A Typical Life Cycle of FPGA-Based I&C System

In development of FPGA-based I&C systems LC (Figure 4) it should be taken into consideration that, from the one side, FPGA-based digital devices are complex software-hardware products, thus having much in common with software. Therefore, in analysis and development of FPGA-based I&C system LC the postulates of software engineering standards are reasonably useful (Kharchenko, V. et al., 2004; Kharchenko, V. et al., 2001; Scott, J., Lawrence, J., 1994).

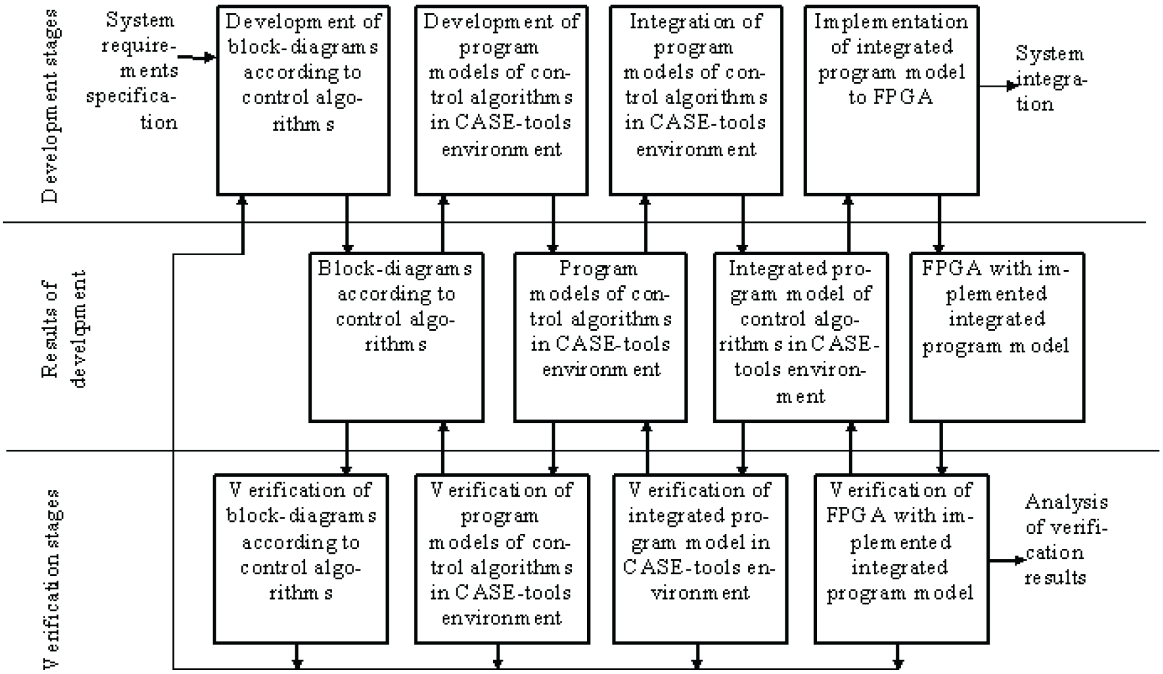
From the other side, FPGA electronic designs as a specific I&C component have some peculiarities different from software. Therefore the postulates of existing standards regulating software structure cannot be mechanically taken for construction of FPGA-project LC.

Our analysis of software LC showed that for FPGA it should study the section of LC beginning from specification of an I&C system and up to its integration. Such actions may be performed in parallel to software development.

Besides, verification after each stage of development is obligatory for both FPGA electronic designs and software. Software verification is a process aimed to confirm software compliance to defined requirements by way of versatile tests and obtaining verifiable proofs (Lyu, M. R., 1996).

FPGA electronic design is developed on the basis of System Requirements Specification (SRS) document with due consideration of function distribution and non-functional safety requirements between FPGAs and other hardware. The developed FPGA-based digital device must be

Figure 4. A life cycle of FPGA-based I&C system


Development stages
Results of develpment
Verification stages
System requirements specification
Development of block-diagrams according to control algorithms
Development of program models of control algorithms in CASE-tools environment
Integration of program models of control algorithms in CASE-tools environment
Implementation of integrated program model to FPGA
System integration
Block-diagrams according to control algorithms
Program models of control algorithms in CASE-tools environment
Integrated program model of control algorithms in CASE-tools environment
FPGA with implemented integrated program model
Verification of block-diagrams according to control algorithms
Verification of program models of control algorithms in CASE-tools environment
Verification of integrated program model in CASE-tools environment
Verification of FPGA with implemented integrated program model
Analysis of verification results

integrated within the I&C system, and in future it should be treated as an integral part of I&C system's software and hardware.

Development of FPGA-based digital devices consists of the following stages:

- Development of signal formation algorithm block-diagrams.
- Development of signal formation algorithm program models in design environment which is determined depending on type and/or manufacturer of FPGA realization environment applied.
- Integration of signal formation algorithm program models (development of digital device integrated program model) into design environment.
- Implementation (loading) of integrated digital device model to FPGA.

The key term here is «signal formation algorithm block-diagram» implying a certain functionally finite project module presented in the form of a graphic diagram or a listing in hardware description language (HDL). The result of each step is a new product, the final result being a FPGA with implemented logic structure. At each step the developed product must be verified. The procedures of FPGA-based I&C system development and verification are shown in Figure 4. A description of FPGA-based I&C system LC stages is presented below.

Development of Signal Formation Algorithm Block-Diagrams: Signal formation algorithm block-diagrams are developed as a direct preparation to development of a digital device block-diagram in CASE-tools (design) environment. Initial data are:

- SRS (functional general and non-functional – general safety requirements) with due consideration of function distribution between software and hardware.
- Process engineering requirements that may be formulated by customer as an addition to SRS requirements.

Initial information in requirements may be both in verbal form and in the form of formalized (problem oriented) languages describing function algorithms.

Signal formation algorithm block-diagrams are developed in the form as close as possible to scheme presentation in FPGA design environment and, as a consequence, should take into consideration the peculiarities of tools applied. For complicated digital devices one of critical issues is structure division into functional modules and formation of series and/or parallel tiers of such modules.

In case the requirements to functioning algorithms are presented in verbal form, at that stage such works may be consecutively performed:

- Development of description of functioning algorithms in a formalized language.
- Development of signal formation algorithm block-diagrams as adapted to current tools.

Development of Signal Formation Algorithm Block-Diagram Program Models in CASE-Tools Environment: The initial data at that stage are signal formation algorithm block-diagrams. Development of signal formation algorithm block-diagram program models in design environment is performed using specialized CASE-tools comprising a library of typical functional elements and blocks.

In the course of development signal formation algorithms and FPGA logic structure are presented in the form of visualized conditional graphic images (block-diagrams). It should be noted that the development of signal formation algorithm block-diagram program models and FPGA program model is similar to the process of software product development in a problem oriented program language using specialized tools.

An alternative to direct diagram drawing may be FPGA structure description in a HDL, such as Verilog or VHDL.

HDL is a formalized record that may be used at all development stages. System function is defined as transformation of input values into output values, operation time in this transform being prescribed in explicit form. General FPGA structure is prescribed by a list of connected components – functional blocks that realize signal formation algorithm block-diagram program models.

At this stage some library modules lacking in standard tools library must be created. Such library modules in FPGA structure are called IP-Cores (Intellectual Property Cores) or IP-functions. Such modules are universal and reliably repetitive, from the one side, and capable of parametric adjustment to a particular project, from the other side. Repeated application of IP-Cores permits to reduce labor costs and design period of digital devices, ensuring their high reliability.

Integration of Signal Formation Algorithm Block-Diagram Program Models in CASE-Tools Environment: At that stage signal formation algorithm block-diagram program models as developed at a previous stage in CASE-tools environment are integrated. An important issue in this is establishment of connections and sequences between developed functional blocks (signal formation algorithm block-diagram program models), including input and output signal formers, in strict conformity with the developed signal formation algorithm block-diagrams.

As well as at the previous stage, integration may be performed both in the form of graphic diagrams and by programming in hardware describing language. The result of this stage is a finite digital device program model ready to be implemented into FPGA chip.

Implementation of Integrated Program Model to FPGA Chip: The developed digital device logic structure program model is implemented by adjustment of connections between FPGA logic cells using the appropriate interface equipment (JTAG interface) connected to an instrumental PC. Interface equipment for adjustment of connections between crystal logic cells is selected in accordance with the type and/or manufacturer of components applied.

Thus, this step is a transfer from software implementation of digital device to its final hardware implementation. The product of this step is an FPGA-based digital device that performs certain functions within I&C system.

Verification Approaches for FPGA Electronic Designs

The conformity between verification stages of FPGA-projects, tasks performed at those stages and methods of task performance is explained in Table 5.

Let us give a short characteristic of FPGA-projects verification methods.

Documentation Technical Review Method Applied to Assess Completeness and Correctness of Algorithm Block-Diagrams: Signal formation algorithm block-diagrams are results (products) of a corresponding FPGA-project development stage. The completeness of signal formation algorithm block-diagrams is assessed by comparison between the lists of developed algorithm block-diagrams to signal formation conditions according to SRS agreed with customer. Conformity criterion is coincidence between the list of developed algorithm block-diagrams and signal formation conditions according to SRS.

Correctness of signal formation algorithm block-diagrams is assessed by correctness, unambiguous treatment and preparation quality of the developed block-diagrams. In the course of analysis the following must be confirmed:

- A separate algorithm block-diagram is presented for each signal formation condition.

Table 5. The conformity between verification stages of FPGA-projects, tasks performed and methods of task performance

Verification Stage	Verification Task	Verification Method
Development of signal formation algorithm block-diagrams	Completeness and correctness assessment of signal formation algorithm block-diagrams	Documentation technical review
	Conformity assessment to SRS	Traceability analysis
	Structuredness assessment of algorithm block-diagrams	Complexity assessment
Development of signal formation algorithm block-diagram program models in CASE-tools environment	Testing of algorithm block-diagram program models	Functional and timing simulation in CASE-tools environment
	Completeness of tests assessment	Walk-through of documentation
	Conformity assessment to algorithm block-diagrams	Traceability analysis
Integration of signal formation algorithm block-diagram program models in CASE-tools environment	Testing of digital device program model	Functional and timing simulation in CASE-tools environment
	Completeness of tests assessment	Walk-through of documentation
	Conformity assessment to program models	Traceability analysis
Implementation of digital device program model to FPGA	Testing of FPGA with implemented program model	Blackbox functional testing
	Completeness of tests assessment	Walk-through of documentation
	Conformity assessment to integrated program model	Traceability analysis

- Each block-diagrams comprises a strict signal formation condition formulation in accordance with SRS.
- Each block-diagram is performed under established form as a connection of typical structural elements selected from a prescribed standard set.
- Inputs and outputs of each structural element are clearly and unambiguously identified in accordance with established rules.
- Identifiers and names are specified for all input signals, alteration limits being also specified for continuous signals.
- Identifiers, names and destinations are specified for all output signals in the scheme.
- Set-points determining signal formation conditions and return to normal operation are specified in the scheme with necessary accuracy.
- Necessary timing characteristics (back offs under alterations of input signals, signal formation delays, signal issuance time before automatic de-energization, etc.) are specified in the scheme with necessary accuracy.

Conformity criterion is meeting all the above requirements to algorithm block-diagrams preparation.

Method of Functional and Timing Simulation in CASE-Tools Environment: Functional and timing simulation in CASE-tools environment implies testing of each of signal formation algorithm block-diagram program models in design environment as well as testing of the integrated program model.

Under functional simulation conditions (“input signals”) corresponding to normal operation and to each of signal formation conditions are consecutively imitated at test inputs. Altered states of program model outputs and/or of established control points within the program model as caused by such effects are observed at instrumental screen and registered as "hard copies" from the screen. Under timing simulation consecutive state alterations at one of program model inputs are imitated in turns and altered states of test outputs ("timing diagrams") and/or of established control points within the program model are monitored.

Tests performed should imply:

- Testing of new functional blocks (IP-Cores), arranged from typical functional elements in CASE-tools environment.
- Testing of algorithm block-diagram program models arranged from typical functional elements and new functional blocks in design environment.
- Testing of integrated algorithm block-diagram program model arranged from signal formation algorithm block-diagram program models in CASE-tools environment.

New functional blocks are tested directly in CASE-tools environment. As the functional blocks are invariant relative to input data, after verification they may be included into the library of CASE-tools applied and find multiple usages during development of FPGA-projects. Tests for algorithm program models are developed on the basis of signal formation algorithm block-diagrams verified at the previous stage.

Tests for integrated program model are developed on the basis of signal formation algorithm program models verified at the previous stage.

The developed tests and testing results must be presented in FPGA-project verification documents in the form of tables and timing diagrams. In timing diagrams the imitated input states (input signals) of program models in CASE-tools environment, their alterations and altered states of each of outputs should be specified.

Criterion of success is a conclusion that test results correspond to expected results.

Walk-through Method of Documentation Viewing Used to Assess Testing Completeness: Walk-through of documentation is a kind of inspection of documents correctness, completeness and consistency. We shall mark the peculiarities of one of the key stages – analysis of testing complete coverage of algorithm program models in the process of FPGA-project verification. Such analysis is performed by comparison between the list of qualitatively different combinations of input states and/or of their alterations that cause altered output states and the list of program model input-output states that are imitated and monitored in the course of testing.

Criteria of conformity in this are:

- Presence and completeness of tests for all new functional blocks composed from typical functional elements.
- Presence and completeness of tests for all FPGA-project algorithm program models.
- PRESENCE AND COMPLETENESS OF TESTS FOR INTEGRATED PROGRAM MODEL.
- Presence and completeness of tests for final FPGA with implemented program model.

Blackbox Functional Testing Method: Functional testing, named also blackbox testing, consists in experimental checking of functions performed by a programmable component with implemented program model to define their conformity to system requirements, signal formation algorithm schemes and user documentation (Scott, J., Lawrence, J., 1994).

Traceability Analysis: This is done to ensure that input requirements of a certain process are exhaustively considered by analysis of their connections to output results as well as all requirements have been defined and brought through the life cycle of development, i.e. from requirement analysis up to final testing.

Traceability analysis includes identification of input requirements and confirmation of the fact that they have been considered by way of inspection of destination documents. For instance, the analysis may inspect translation of system requirements documentation into FPGA-project requirements documentation, or that of FPGA-project requirements documentation into digital device characteristic specification, or that of system requirements documentation into tests, etc. If necessary, traceability analysis may include a requirements confirmation step to ensure that actual requirements, but not simply sections of input documentation, have been traced. The results of analysis must show whether all requirements have been duly considered. For this analysis usually traceability matrices are used comprising comparison between input requirements and the elements of output results.

In the course of FPGA-projects verification traceability analysis is applied to ensure tracing or establishment of connections:

- Between SRS and signal formation algorithm block-diagrams.
- Between signal formation algorithm block-diagrams and their program models in CASE-tools environment.
- Between signal formation algorithm block-diagrams and integrated program model in CASE-tools environment.
- Between FPGA electronic designs integrated program model in CASE-tools environment and FPGA with implemented logic structure.

Conformity of signal formation algorithm block-diagrams to the initial data of SRS is assessed for each block-diagram separately by comparing:

- Logic conditions of signal formation and return to normal operation, the latter being defined by this scheme, to conditions established in specification.
- Numerical values of set points and timing characteristics that define conditions of signal formation and return to normal operation to their values established in specification.
- Identifiers and names of input and output signals and alteration limits of continuous input signals as specified in the scheme to specification data.

Conformity criterion for this verification stage is coincidence of logic conditions, numerical values of set points and timing characteristics, identifiers, names and alteration limits of signals as defined from signal formation algorithm schemes to initial data established in specification.

Conformity of algorithm program models developed in CASE-tools environment to signal formation algorithm block-diagrams is assessed by way of comparison:

- Of identifiers, names and alteration limits of input signals.
- Of identifiers, names and formation logic conditions of output signals.
- Of connection topologies between structural elements, numerical values of set points and timing characteristics specified in algorithm block-diagrams and “hard copies” from screen that diagrammatically reflect the developed algorithm program models.

Conformity criteria for this stage are:

- Usage in algorithm program models of only those elements that are included into typical functional elements library of CASE-tools environment applied.
- Presence and completeness of tests for all new functional blocks composed from typical functional elements.
- Presence and completeness of tests for all algorithm program models.

- Positive testing results of all new functional blocks and algorithm program models in CASE-tools environment applied.
- Equivalence of developed algorithm program models and protective signal formation algorithm block-diagrams as verified at previous stage.
- Absence of any input, output signals and/or set points in FPGA electronic design model for which inputs and/or outputs exist in none of algorithm program models.

Conformity of FPGA with implemented program model to this program model in CASE-tools environment is assessed by comparison of signal formation conditions and timing characteristics as obtained by testing to logic conditions, numerical values of set points and timing characteristics specified in algorithm block-diagrams and "hard copies" from screen that diagrammatically reflect the developed FPGA logic structure program model.

Conformity criteria for this verification stage are:

Successful implementation of FPGA electronic design that was verified at previous stage into FPGA-chip.

Equivalence of output signal formation conditions and timing characteristics as obtained by testing to logic conditions, numerical values of set points and timing characteristics of FPGA electronic design that was verified at previous stage.

Thus, FPGA electronic design traceability analysis method for each verification stage includes such actions:

- Analysis of verification stage input data presentation and separation of component classes (signals, communication lines, nodes, functional blocks, etc.)
- Detailed analysis of components in each class.
- Filling of traceability matrix with input data by systematization of components in each class.
- Analysis of verification stage output data presentation and separation of component classes.
- Conformity analysis between input and output data and filling of traceability matrix with output data by comparison of each of output data component and input data components.
- Analysis of final traceability matrix, formulations of conclusions and recommendations.
- Overpatching and correction of final product in case any discrepancies are found between input data and output result of development stage.

Let us prepare a formal description of FPGA electronic design traceability analysis.

FPGA electronic design is developed and verified in 4 stages, with traceability analysis performed for each stage. Assume FPGA realizing N signal processing algorithms. For each algorithm S classes of omponents exist that belong to FPGA algorithm as well as L input components Aij of FPGA algorithm and M output components Bij of FPGA algorithm that belong to i-th class. Our analysis shows that component classes of FPGA algorithms are equivalent for each development class. Between all input and output algorithm component we must ascertain whether equivalence conformity is met or not. In this context traceability analysis would be successful if each of input elements corresponds to one or more output elements and each of output elements corresponds to one or more input elements:

$$(\forall A_{ij} : \exists\left\{B_{ij}\right\}, A_{ij} \Leftrightarrow \left\{B_{ij}\right\}) \vee (\forall B_{ij} : \exists\left\{A_{ij}\right\}, B_{ij} \Leftrightarrow \left\{A_{ij}\right\}). \quad (1)$$

In case condition (1) is not met, input and output data of a development stage are not intertraceable and stage results mist be corrected.

Traceability matrix includes four columns:

1. **Column of FPGA Algorithm Input Components:** Its elements are input components A_{ij}, i = 1,...,S, j = 1,...,L.
2. **Column of FPGA Algorithm Output Components:** Its elements are output components B_{ij}, i = 1,...,S, j = 1,...,M.
3. **Column of Traceability Results:** Elements are conclusions of traceability between FPGA algorithm input and output components; conclusion data take binary values "meeting" ($A_{ij} \Leftrightarrow B_{ij}$ met) or "not meeting" ($A_{ij} \Leftrightarrow B_{ij}$ not met).
4. **Column of Comments:** Additional data on FPGA algorithm components development and verification.

Complexity Assessment: One of basic FPGA electronic designs characteristics affecting their reliability is complexity. FPGA electronic design complexity metrics may be applied to access the critical scope of signal formation algorithms and integrated program model, above which the probability of bringing errors drastically increases. Complexity assessment includes (McCabe, T. A., 1976):

- Analysis of problem oriented language in which the algorithms have been developed, separation of operator and operand classes.
- Prescription of weights from the point of view of complexity for operator and operand classes.
- Establishment of limit value for integral complexity metric above which the probability of bringing errors into FPGA electronic designs drastically increases.
- Direct complexity measurement including count of the number of operators and operands for each class and determination of integral complexity metric value.
- Analysis of obtained complexity metric values, formulation of conclusions and recommendations.
- Breaking into modules for those algorithms where complexity metric exceeds its limit value.

Key Advantages of FPGA Technology

FPGA is a convenient technology not only for implementation of auxiliary functions (transformation and preliminary processing of data, diagnostics, etc), it is also effective for implementation of safety important NPP I&Cs control functions. Application of the FPGA technology is more reasonable than application of software-based technology (microprocessors) in many cases (Kharchenko, V. S., 2008).

The application of FPGA technology has significant advantages that can be utilized both in I&C modernization projects of existing NPPs and in I&C designs for new NPPs. These advantages are the following:

- Design, development, implementation, and operation simplicity and transparency.
- Reduction of vulnerability of the digital I&C system to cyber attacks or malicious acts due to absence of any system software or operating systems.
- Faster and more deterministic performance due to capability of executing logic functions and control algorithms in a parallel mode.
- More reliable and error-free end-product due to reduction in the complexity of the verification and validation (V&V) and implementation processes.
- Relatively easy licensing process of FPGA-based safety systems due to the simplicity and transparency of system architecture

and its design process and possibility to provide evidence of meeting licensing requirements, such as independence, separation, redundancy and diversity, in an easier and more convincing way.

- Resilience to obsolescence due to the portability of the HDL code between different versions of FPGA chips produced by the same or different manufacturers.
- Possibility of reverse engineering results implementation via emulation in FPGA of obsolete central processing unit (CPU) without modification of existing software code.
- Specific beneficial properties regarding cyber security compared to microprocessors (no viruses for FPGA).

The following FPGA features are important for safety and dependability assurance:

- Development and verification are simplified due to apparatus parallelism in control algorithms implementation and execution for different functions, absence of cyclical structures in FPGA projects, identity of FPGA project presentation to initial data, advanced testbeds and tools, verified libraries and IP-cores.
- Existing technologies of FPGA projects development (graphical scheme and library blocks in CAD environment; special hardware describing languages VHDL, Verilog, Java HDL, etc; microprocessor emulators which are implemented as IP-cores) allow increasing a number of possible options of different project versions and multi-version I&Cs.
- Fault-tolerance, data validation and maintainability are improved due to use of: redundancy for intra- and inter-crystal levels; possibilities of implementation of multi-step degradation with different types of adaptation; diversity and multi-diversity implementation; reconfiguration and recovery in the case of component failures; improved means of diagnostics.
- FPGA reprogramming is possible only with the use of especial equipment (it improves a security); stability and survivability of FPGA projects are ensured due to the tolerance to external electromagnetic, climatic, radiation influences, etc.

FPGA-BASED NPP I&CS

This section provides information on FPGA-based NPP I&Cs by the example of systems produced by RPC Radiy.

RPC Radiy developed the RadICS FPGA-based platform, which comprises a set of general-purpose blocks that can be configured and used to implement application-specific functions and systems. The RadICS platform is composed of various standardized modules, each based on the use of FPGA chips as computational engines.

RadICS-based I&C systems provide extensive on-line self-surveillance and diagnostics at various levels, including self-diagnostic and defensive coding of electronic design components, self-monitoring of FPGA circuits, such as control of FPGA power, watchdog timer, cyclical redundancy check (CRC) calculation, state monitoring, and monitoring the performance of FPGA support circuits, I/O modules, communications units, and power supplies.

RadICS-Based Applications

I&C systems based on the FPGA-based platforms produced by RPC Radiy include the most critical and high-reliability applications in NPPs, such as Reactor Trip, Reactor Power Control and Limitation, Engineered Safety Features Actuation, and Rod Control. Other examples include Nuclear

Island Control Systems, Turbine Island Control Systems and Automatic Regulation, Control, Operation and Protection (ARCOP) of Research Reactor.

Reactor Trip System (RTS): The RTS continuously monitors the actual values of neutron flux and other process variables, and it conditions shutdown signals in case these variables reach their setpoints. RTS transmits all vital information necessary for surveillance and monitoring to the control room and other safety and non-safety systems (e.g., initiation status, plant and diagnostic data). RTS can have 3 or 4 redundant channels depending on the design basis of the nuclear reactor, and it can implement a voting logic of two-out-of-three (2oo3) or two-out-of-four (2oo4). Example of 2oo3 configuration is shown in Figure 5. The external interfaces of the RTS provide interfaces to power supplies, process I/Os, communication links, local inputs, and indicators.

A typical RTS (see Figure 6) has on-line monitoring and maintenance capabilities. It can correct its voting logic in case faults are detected, so that system availability is optimized without compromising safety. RTS has a self-diagnostic subsystem, which includes troubleshooting assistance functions for easy localization of faults. In case of failure, RTS puts itself in the safe state, signalling actuation for shutdown. RTS also supports manual actuation of shutdown logic from the Main Control Room (MCR) or Emergency Control Room (ECR). The FPGA-based RTS architecture can be adapted to various reactor types (e.g., PWR, BWR, PHWR).

There are 28 RTSs produced by RPC Radiy in operation at Zaporozhe NPP, Rovno NPP, Khmelnitsky NPP and South-Ukrainian NPP.

Reactor Power Control and Limitation Systems (RPCLS): RPCLSs (Figure 7) perform the following main functions:

Figure 5. Reactor trip system configuration (2oo3 voting logic version)

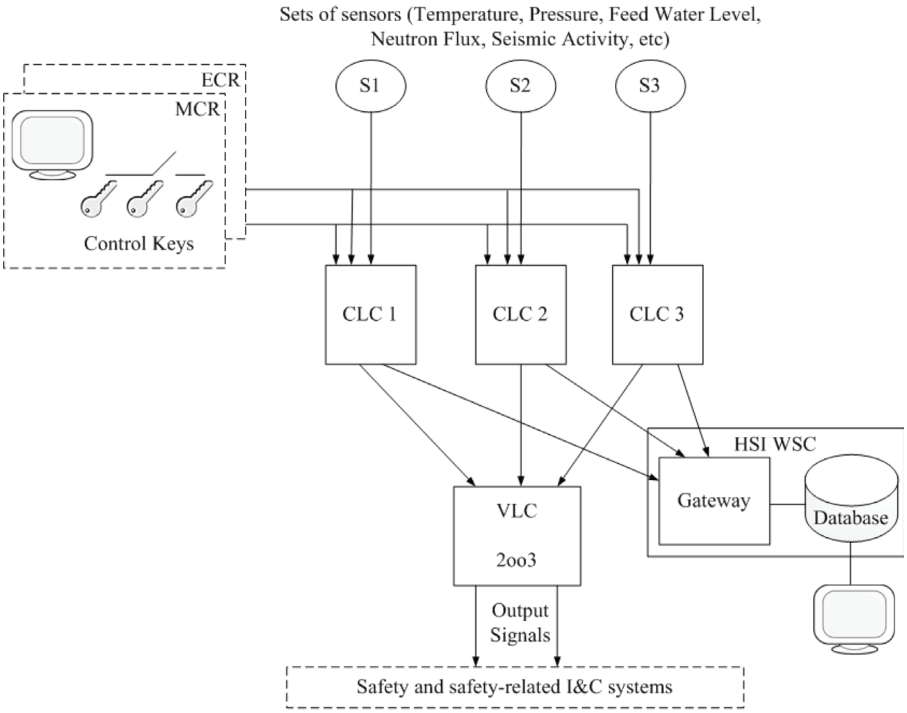

Sets of sensors (Temperature, Pressure, Feed Water Level, Neutron Flux, Seismic Activity, etc)
ECR
MCR
Control Keys
S1
S2
S3
CLC 1
CLC 2
CLC 3
HSI WSC
Gateway
Database
VLC
2oo3
Output Signals
Safety and safety-related I&C systems

Figure 6. Reactor trip system

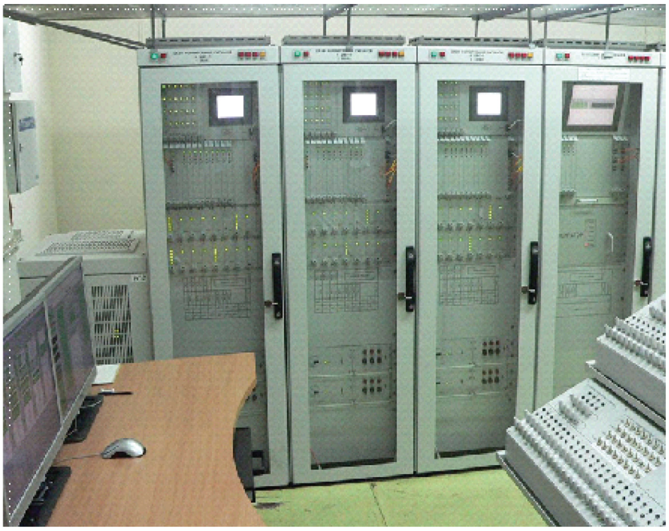
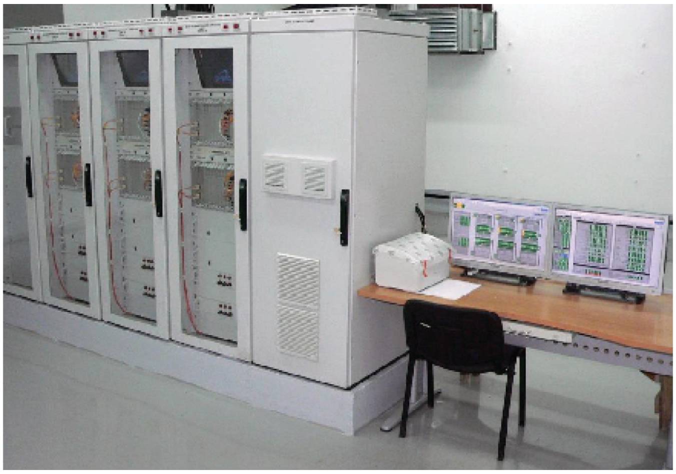


Figure 7. Reactor power control and limitation system



- Automatic and continuous regulation of reactor neutron power and/or pressure in the main steam line of NPP power unit turbine.
- Control of reactor power at levels corresponding to the range of NPP power unit main licensing limitations, from start up through full-power operation.
- Fast-responding preventative protection of the reactor (runback at 40-50% of full power within 3 to 4 seconds).

To increase the reliability of the protection functions, output signals implement in a 2oo3 voting logic. If licensing schemes require, the system can be designed in a 2oo4 configuration with full reliability and quality compliance.

During the design phase of any specific RP-CLS, divisional principles are implemented within the control and protection functions. In order to achieve high reliability and independences, different groups of protection functions are realized in separate galvanically isolated subunits.

From 2004 to 2012, nine Reactor Power Control and Limitation Systems were put in operation in Ukrainian NPPs.

Rod Control System (RCS): The RCS (Figure 8), in general, consists of Rods Position Indication System / Subsystem (RPIS) and Rods Drives Control System / Subsystem (RDCS) with control logic processing equipment power supply subsystem and also can include its own Rod Drives Electric Power Supply Subsystem (RDEPSS) made by RPC Radiy (or any other type of RDEPSS).

RPIS can indicate all reactor control and safety rods position operation parameters and real rods position. RDCS performs all Rod Drives control functions and include Trip Portion (set of the Rod Drives power supply breakers).

RDEPSS provides the following functions:

- Uninterrupted electric power supply of Rod Drives in normal operation mode.
- Switching off the Rod Drives electric power supply by Emergency Protection (EP) signals in case of normal operation failure which requires placing the reactor into a subcritical state.

RCS can have 2 or 3 redundant channels depending on the design basis of the nuclear reactor, and it can implement a voting logic of 1oo2 or 2oo3. Generic architecture of RCS configuration in 1oo2 voting logic version for PWR Unit is shown in Figure 9.

In 2012, the first full set of RCS has been successfully put in operation in the Unit 1 of the South-Ukrainian NPP with WWER-1000 PWR-type reactor.

Engineered Safety Features Actuation System (ESFAS): The ESFAS (see Figure 10) produced by RPC Radiy executes the following main functions:

- Protection, interlocking and monitoring of the automated operation of actuators.
- Automatic process control.
- Manual remote control of actuators.

The ESFAS also provides the implementation of functions that are necessary for NPP safety:

- Information and data acquisition.
- Signal conditioning and control of safety signals, detectors, and sensor.
- Full-scope systems diagnostics.

The following design principles are applied in the ESFAS:

- Diversity of input signals (e.g., current, voltage, resistance, “dry contact”).

Figure 8. Rod control system

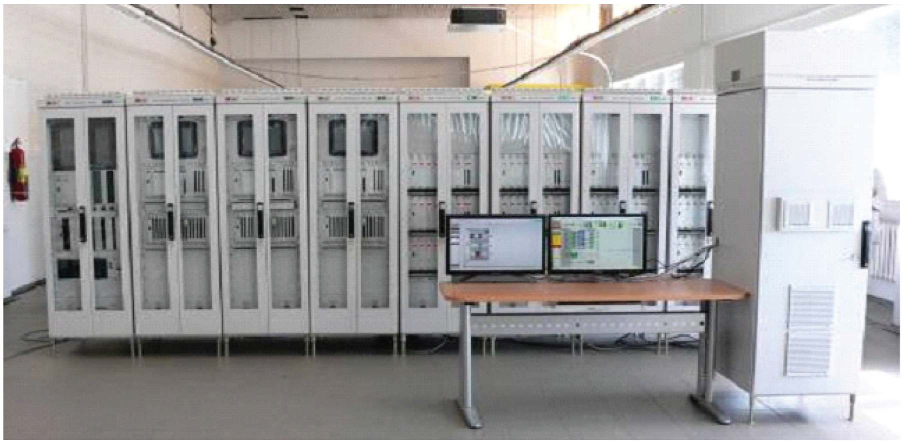
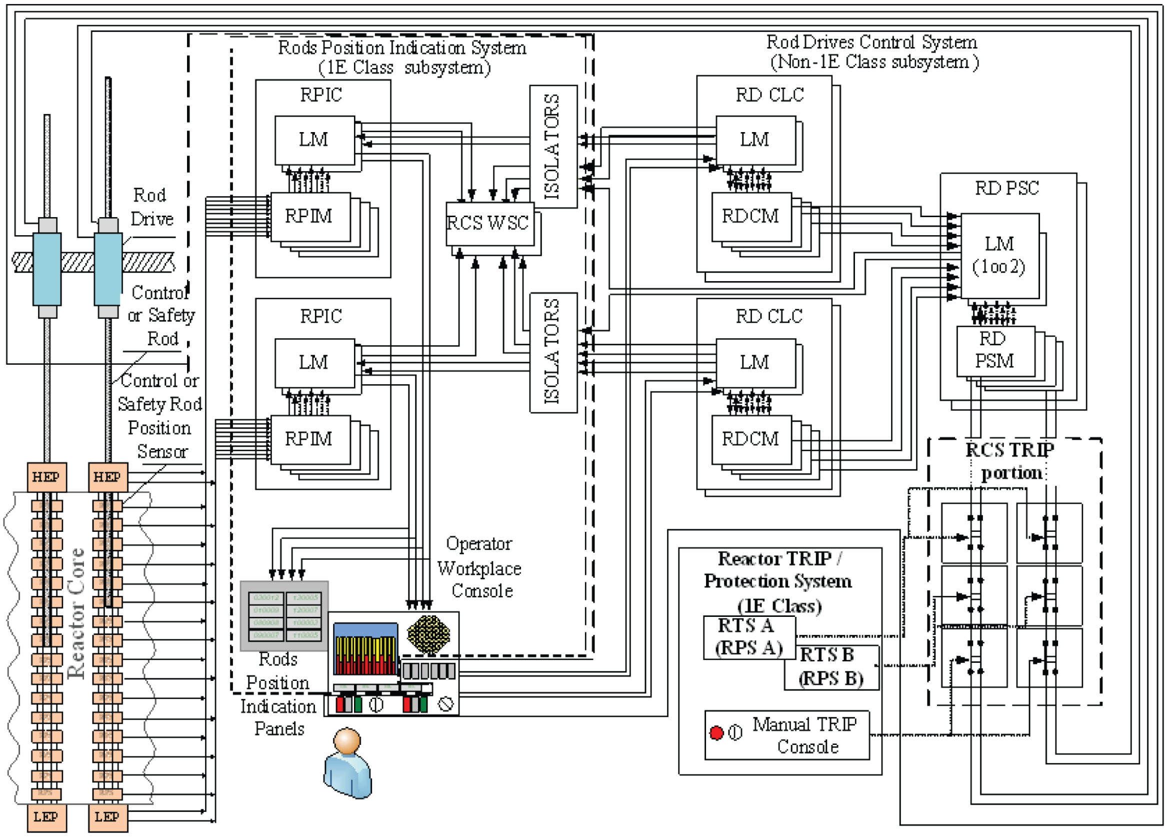


Figure 9. Generic architecture of RCS configuration in 1oo2 voting logic version for PWR Unit



- ◦ System size scalability accommodating needs for increased number of inputs and outputs.
- ◦ Simple and controlled ways of code modification of protection, interlocking and control algorithms.
- ◦ Adaptability of interfacing capabilities for communication and integration with other control, monitoring and regulating systems.

The ESFAS can be supplied in single-, two-, three-, or four-channel installations. The ESFAS conforms to safety class 2, can be designed and built in accordance with applicable national standards in the EU countries and the USA.

Eighteen ESFASs are in operation now at Rovno NPP, South-Ukrainian NPP, and Kozloduy NPP (Bulgaria).

Nuclear Island and Conventional (Turbine) Island Systems: Nuclear Island and Conventional (Turbine) Island Systems (see Figure 11) have the following main functions:

- Conditioning and initiation of protection, interlocks and alarm commands.
- Conditioning and initiation of automatic regulation commands when process values deviate from setpoints.
- Initiation of remote control commands based on operators' instructions.
- Indicate current states, positions and operating modes of actuators in control rooms.

Figure 10. Engineered safety features actuation system

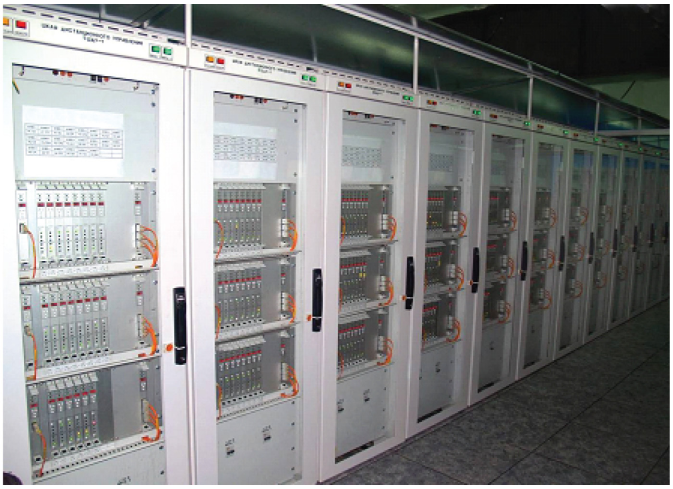
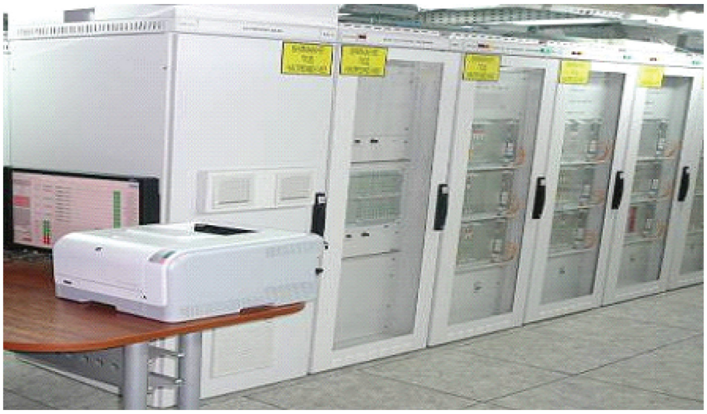


Figure 11. Nuclear island system



There are five Nuclear Island and Conventional (Turbine) Island Systems in operation now at Ukrainian NPPs.

Automatic Regulation, Control, Operation and Protection for Research Reactors (ARCOP): ARCOP system is designed to implement safe operation of research reactors. ARCOP performs the following functions:

- Measurement and monitoring of neutron physical reactor parameters.
- Measurement and monitoring of thermal physical parameters.
- Generating the emergency protection and preventative signalling.
- Automatic reactor power regulation.
- Remote and automatic control of actuators.
- Diagnostics and information display support.

In 2006, an ARCOP system was installed at the WWR-M type research reactor in the Institute of Nuclear Research at the National Science Academy of Ukraine, Kiev.

ANALYSIS ASPECTS OF FPGA-BASED NPP I&C SYSTEMS

Verification and Validation of FPGA-Based NPP I&Cs

FPGAs were first introduced in non-safety systems in NPPs, where no specific process over general FPGA development process is required. However, to use FPGAs for safety systems, more strict processes are imposed by nuclear regulators to ensure the reliability and safety of the systems.

Since the development process of FPGA is similar to that of software for microprocessor-based systems, the conventional safety software development process including V&V methods can be applied. I&C systems supplied by the RPC Radiy were subjected to V&V processes to ensure their reliability and safety.

For example, for US commercial NPPs, the US NRC endorses IEEE Standard 7-4.3.2-2003 as the methods for high functional reliability and design requirements for computers, whereas IEEE Standard 1012-1998 as the methods of V&V.

IEEE Standard 1012-1998 postulates a phased software life cycle, and defines a number of V&V activities to be performed throughout the software lifecycle. The V&V activities include the following types of activities:

- Software requirements evaluation.
- Design evaluation.
- Interface analysis.
- Requirements traceability analysis.
- Source code and source code documentation evaluation.
- Validation testing.
- Hazard analysis.

Combined Usage of Analysis Techniques

There are a lot of well-known techniques that can be used for NPP I&CS dependability analysis and assessment of its attributes. Using these techniques it is possible to perform quantitative and/or qualitative assessments. Qualitative assessments though lacking the ability to account, are very effective in identifying potential failures within the I&CS. We have performed some work to identify possible combination of techniques, results are shown in Figure 12. To carry out dependability analysis it is necessary to have I&CS technical documentation (this information is obtained from I&CS project) and reliability data of I&CS components (is obtained from component vendors).

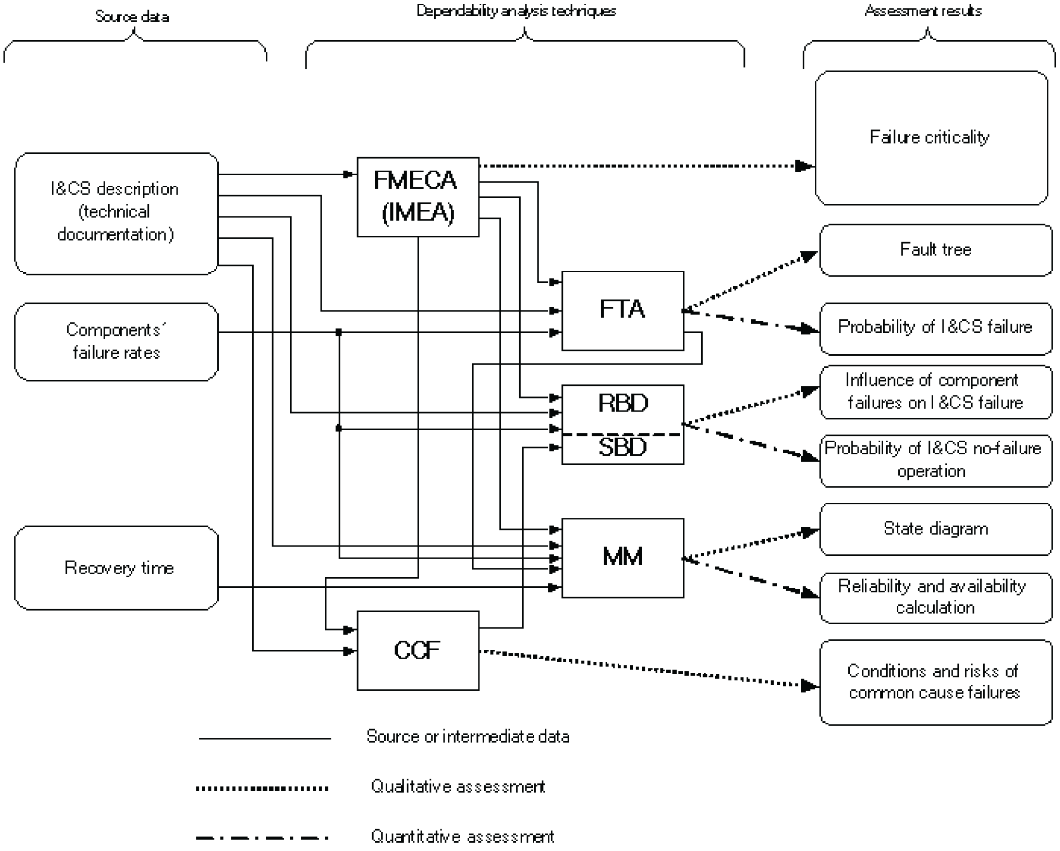
The first stage of NPP I&CS dependability analysis is FMECA (Failure modes, effects and criticality analysis). During this stage all possible failure mechanisms and failure rates for all components involved and quantify failure contribution to overall NPP reliability and safety are analyzed.

In FMECA qualitative and quantitative results (see Figure 13) are obtained. Failure mode in FMECA refers to the way a failure might occur. Failure effect is the consequence of failure from the system's point of view. Failure criticality is assigned to each failure mode to get quantitative parameters.

FMECA is carried out early in the NPP I&CS development life cycle to find ways of mitigating failures and thereby enhancing reliability through design.

A traditional FMECA uses potential component failures as the basis of analysis. Component failures are analyzed one by one, and therefore important combinations of component failures might be overlooked. Environmental conditions, external impacts and other such factors are ana-

Figure 12. Combined usage of dependability analysis techniques


Source data
Dependability analysis techniques
Assessment results
I&CS description (technical documentation)
Components' failure rates
Recovery time
FMECA (IMEA)
FTA
RBD
SBD
MM
CCF
Failure criticality
Fault tree
Probability of I&CS failure
Influence of component failures on I&CS failure
Probability of I&CS no-failure operation
State diagram
Reliability and availability calculation
Conditions and risks of common cause failures
Source or intermediate data
Qualitative assessment
Quantitative assessment

lyzed in FMECA only if they produce component failures; external influences that do not produce component failures (but may still produce I&CS failure) are often overlooked.

That's why it is not sufficient to use only FMECA during NPP I&CS analysis.

To take into account external impacts it is possible to use IMEA (Intrusion Modes and Effects Analysis). IMEA is a modification of FMECA that takes into account possible intrusions to the system, examples of this analysis are shown in (Babeshko, E. et al., 2010; Babeshko, E. et al., 2011).

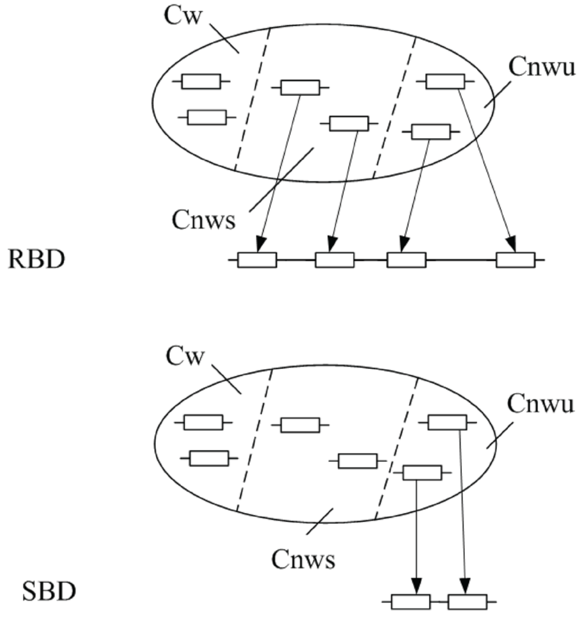
Results of FMECA and IMEA are used during further FTA (Fault Tree Analysis), RBD / SBD (Reliability/Safety Block Diagram), CCF (Common Cause Failure Analysis), and also during Markov modeling.

Reliability block diagram (RBD) is a graphical analysis technique, which expresses the concerned system as connections of a number of components in accordance with their logical relation of reliability. Safety block diagram (SBD) is a similar technique that treats safety aspects.

Figure 13 shows RBD and SBD principles. Set of NPP I&CS components is split into the following groups:

- Components that can't lead to NPP I&CS failure Cw.
- Components that can lead to I&CS failure, but system state would be safe Cnws.
- Components that can lead to I&CS failure, but system state would be unsafe Cunws.

Figure 13. Reliability and safety block diagrams: principles of development



While RBD treats all possible failures (both Cnws and Cnwu are included into RBD), SBD treats only components that can lead to unsafe situation (only Cnwu are included). That gives possibility to concentrate on safety aspect and to simplify all following calculations.

During RBD (SBD) it is possible to use list of all components that can cause I&C system failure which has been obtained during FMECA. Then we take into account I&CS architecture (number of components, software and hardware versions, type of diversity, check and reconfiguration means) and sets of different faults and calculate reliability and safety indicators.

FMECA results are used in FTA to get list of all possible failures.

To perform Markov modeling it is required to know component's failure rates and recovery time so as to get state-to-state transitions. In most cases the NPP I&CS operation may be analyzed using a Markov model.

Solution and Recommendations

Nowadays FPGAs are widely used in different fields, including critical ones, and there is a trend that situation will remain like this in the nearest future. Therefore, it is necessary to work at reliability and safety analysis of FPGA-based systems.

Experience shows that combined usage of analysis methods provides better results, therefore such approach should be developed further.

A problem of assessment and assurance for safety important I&C systems is still challenging due to the fact that such systems consist of interconnected complex components with different functions and different nature; moreover, the majority of modern I&C systems are being FPGA-based, hence, it is impossible to perform their assessment without consideration of all the special features for all the technologies used.

This approach implies identification of all possible discrepancies, on the basis of product and life cycle processes, and their assessment via application of FMECA, FTA, IMECA and other techniques.

FUTURE RESEARCH DIRECTIONS

More detailed analysis of advantages and risks of FPGA technology application should be fulfilled taking into account an experience of companies (similar RPC Radiy) producing and implementing FPGA-based NPP I&C systems. Proposed approaches can be strengthened by development of support tools that will allow to automate analysis process.

The future research and development directions are the following:

- Development of a tool that supports joint application of the different techniques (RBD, FMECA, gap analysis).
- Implementation of tool-based calculation of metrics for choosing the optimal set of applicable methods to ensure reliability and safety of FPGA-based I&C systems.

CONCLUSION

Nowadays, FPGA-based platforms are used in I&C modernization projects at various NPPs for a wide range of safety and control functions and systems, such as reactor trip system, reactor power control and limitation system, engineered safety features actuation system, rod control system, nuclear island control system, and turbine island control system.

The above applications represented large-scale modernization projects, however, the technology can provide solutions for an even larger variety of applications, such as 'pin-to-pin' or like-for-like type replacement of obsolete circuit board components, reverse engineering, emulation of functions performed by obsolete computers, replacement of components and sub-systems, and building full I&C systems or diverse back-up systems in new NPP designs. FPGA technology allows implementing any safety and control functions that are typical in existing NPPs or in any new designs, therefore providing a technology-neutral implementation tool.

REFERENCES

Babeshko, E., et al. (2009). Extended dependability analysis of information and control systems by FME(C)A-technique: Models, procedures, application. In *Proceeding of IEEE DepCoS RELCOMEX Conference*. IEEE.

Babeshko, E., et al. (2010). Approaches to NPP I&C systems dependability assessment: Analysis and implementation. In *Proceedings of International Congress on Advances in Nuclear Power Plants* (ICAPP. '10). ICAPP.

Babeshko, E. et al. (2011). Combined implementation of dependability analysis techniques for NPP I&C systems assessment. *Journal of Energy and Power Engineering*, *5*(42), 411–418.

Barkalov, A. et al. (2006). *Design of control units with programmable logic*. University of Zelena Gura.

Kharchenko, V., et al. (2001). Methodology of NPP I&C system algorithms and software veri-fication expert analysis. In *Proceedings of Workshop on Licensing and Operating Experience of Computer-Based I&C Systems*. Hluboka-nad-Vltavou, Czech Republic: Academic Press.

Kharchenko, V., et al. (2004). The technique and the experience of expertise of software for NPP: Instrumentation and control systems. In *Proceeding by 7th International Conference on Probabilistic Safety Assessment and Management and European Safety and Reliability Conference*. Berlin, Germany: Academic Press.

Kharchenko, V. S., & Sklyar, V. V. (Eds.). (2008). *FPGA-based NPP instrumentation and control systems: Development and safety assessment. Research and Production Corporation Radiy, National Aerospace University named after N.E. Zhukovsky KhAI*. State Scientific Technical Center on Nuclear and Radiation Safety.

Lyu, M. R. (1996). *Handbook of software reliability engineering*. New York: McGraw-Hill Company.

McCabe, T. A. (1976). Complexity measure. *IEEE Transactions on Software Engineering*, *4*(2), 308–320. doi:10.1109/TSE.1976.233837

Melnyk, A., et al. (2007). Automatic generation of ASICS. In *Proceedings of NASA/ESA Conference on Adaptive Hardware and Systems*. Edinburgh, UK: NASA/ESA.

Scott, J., & Lawrence, J. (1994). *Testing existing software for safety related applications*. Lawrence Livermore National Laboratory.

Tam, S. (2003). *Error detection and correction in virtex-II pro devices*. Application Note: Virtex-II Pro Family. XAPP645 (v1.1).

ADDITIONAL READING

Sakharwade, C. (2008). *Designing FPGA based systems for industrial automation* (pp. 1–19). Latest Technologies and Tools in Electronic Design. doi:10.1049/ic.2008.0764

Simpson, P. (2010). *FPGA Design*. Best Practices for Team-based Design. doi:10.1007/978-1-4419-6339-0

Vanderbauwhede, W., & Benkrid, K. (2013). *High-Performance Computing Using FPGAs*. doi:10.1007/978-1-4614-1791-0

KEY TERMS AND DEFINITIONS

FPGA (Field Programmable Gate Array): A programmable complex electronic component which includes two entities: FPGA chip and FPGA electronic design.

FPGA Electronic Design: A set of statesments in HDL which is appropriate for implementation in FPGA chip.

HDL (Hardware Description Language): A specialized computer language used to describe the structure, design and operation of digital logic circuits.

IP Core (Intellectual Property Core): Is a reusable unit of logic, cell, or chip layout design that can be used as building blocks within ASIC chip designs or FPGA logic designs.

JTAG: Is an integrated method for testing interconnects on printed circuit boards that are implemented at the integrated circuit level.

Logic Synthesis: A process by which an abstract form of desired circuit behavior is turned into a design implementation in terms of logic gates.

LUT: The key component of modern FPGAs that is used to encode any n-input Boolean function by modeling such functions as truth tables.

Chapter 5
Software of Safety Important I&C Systems

Vyacheslav Kharchenko
National Aerospace University named after N.E. Zhukovsky KhAI & Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Vladimir Sklyar
Research and Production Corporation Radiy, Ukraine

Andriy Volkoviy
Samsung Electronics Ukraine Company LLC, R&D Center, Ukraine

ABSTRACT

Features of software as a component of Instrumentation and Control (I&C) systems are analyzed. Attention is paid to the importance of functions performed by software and hazards of such software. Requirements for characteristics of software as a component of I&C systems are analyzed. Different regulatory documents are considered in order to disclose common approaches to the use of dedicated software and off-the-shelf software components. Classification of software, as well as classification of requirements, is described. Criteria of selection and structuring of requirements, as well as criteria for software verification, are defined. As long as the characteristics of software components directly depend on the quality of the processes of software development and verification, requirements for software life cycle processes are considered. The second part of this chapter is dedicated to evaluation of software for nuclear power plant I&C system. Criteria and principles of evaluation are observed. Evaluation of the characteristic of software as a product and software development and verification processes are considered.

INTRODUCTION

Regardless of the purpose and application area any modern digital systems has software as integral part of the system. Instrumentation and control systems are not exceptions and may include software in many various forms: firmware and embedded software (written for particular hardware and usually executed without an operating system), system software (e.g. operating systems and platforms), middleware and device drivers, application software (typically written to be run under operating systems and usually interact with users), configuration for FPGA devices,

DOI: 10.4018/978-1-4666-5133-3.ch005

etc. Software of different forms and types has specific properties. Moreover functions that are performed by software impose constraints on both software as a product and software lifecycle as a processes. For example, use of operating systems and application software has a very limited scope in safety important systems.

In the context of safety important I&C systems, increase in portion of software-produced or software-supported functions requires more attention to software. In this chapter software (SW) for nuclear power plant's (NPP) instrumentation and control (I&C) systems is concerned. That means that references to specific regulations for nuclear power engineering are given, particular terminology and classifications are used.

BACKGROUND

The increase of the number of nuclear power plant I&C software executed functions causes an increase of the "weight" of software device defects and its possible sources of failures. Based on different estimates such defects cause up to 70% of the failures of computer systems of critical application complexes, of the total number of those attributed to nuclear power plant I&C systems (Everett, 1998) (Lyu, 1996). Given this, the present trend is having an increasing dynamic role over time.

In the 1960s software defects caused up to 15% of the failures, and in the 1970s it was 15-30%, and by the year 2000 they were the cause of up to 70% of computer system failures. This trend shows up even more in space rocket technology (Aizenberg, 2002). Analysis of the cause of accidents and catastrophes of space rocket systems, where on board and ground computer systems have already been in use for several decades, allows one to determine that in the past 40 years each fifth accident is related to failure of a digital control system. Six of seven failures of these systems were caused by the occurrence of software defects. One such defect of computer software of the Ariane-5 navigational system in 1997 led to an accident which cost nearly one half billion dollars (Adziev, 1998). In nuclear power generation programmable I&C systems have had a shorter history, however, here also there have been accidents due to software defects.

The reliability of software, as for the I&C system as a whole, depends on the design quality at stages that directly precede development of the software:

- Development of requirements for I&C system.
- Mathematical models.
- Software created functioning algorithms.

Errors committed at these stages become sources of complex defects in software. In this sense, software, on the one hand, accumulates the deficiencies of the preceding stages, and on the other hand, is the "field," in which they can show up and be eliminated. However, the efforts that must be made to do this, increase by an order of magnitude.

Consequently, software is becoming an even more important factor determining the safety of nuclear power plant I&C system. This explains the fact that software of nuclear power plant I&C system, in accordance with national and international normative documents, is a separate and very important object of safety standardization.

SOFTWARE OF NUCLEAR POWER PLANT I&C AS AN OBJECT OF SAFETY REQUIREMENT ESTABLISHMENT

Aspects of Software in Establishing Safety Requirements

Software has a number of important features that should be taken into account in establishing requirements for it. The main of these features are listed below.

1. On the one hand, software is a component of I&C system and shall comply with general requirements for the system, and on the other hand it is an independent and specific object for establishment of requirements, which is confirmed by a large number of international and national standards and methodological normative documents completely devoted to software.
2. Defects that are committed during the development and are not revealed during software verification, can be actuated under certain conditions in the I&C system operating process and lead to their failure. This failure cannot be compensated even if redundant channels are available. If that channels use identical software versions, software defects are in all channels and reveal themselves simultaneously leading to the same kind of distortion of information at the outputs. Therefore, software defects are potential and quite likely source of common cause failure. For this reason, on the one hand software requirements include both requirements for its characteristics (structure, functions and properties) and software lifecycle processes; on the other hand there is a requirement for whole I&C system related to adherence of diversity principle, that is addressed primarily to software, because the use of several program copies increases the likelihood of failures and faults, caused by their hidden defects.
3. At different stages of the software lifecycle (primarily design, coding, integration and testing) different tools are widely used. These tools are also software products, which are intended to reduce the number of defects and increase the reliability of I&C software. However, defects can also be introduced into the I&C software through the software tools. It is the common approach when control systems are based on programmable logic controllers (PLC) for which specialized computer-aided design (CAD) tools are used, and in view of the complexity of such CAD tools both intrinsic defects of a tool and improper use of a tool can be the source of I&C software defects. Therefore, requirements for software must include requirements for software tools used in development and verification.
4. Because documentation is an integral part of software, the requirements for I&C software also include requirements for documentation that is used at all stages of the lifecycle.
5. Software must be examined not only as an independent object of safety standardization, but as a necessary means that will ensure conformity of the I&C system to requirements established for it with regard to redundancy, maintainability, technical diagnostics and so forth.
6. Software requirements are not permanent. The experience with creation and use of I&C system as well as improvement of the information technologies lead to the necessity to improve the requirements. Therefore, requirements must reflect basic and most stable situations considering this experience and prospects of software development technologies.

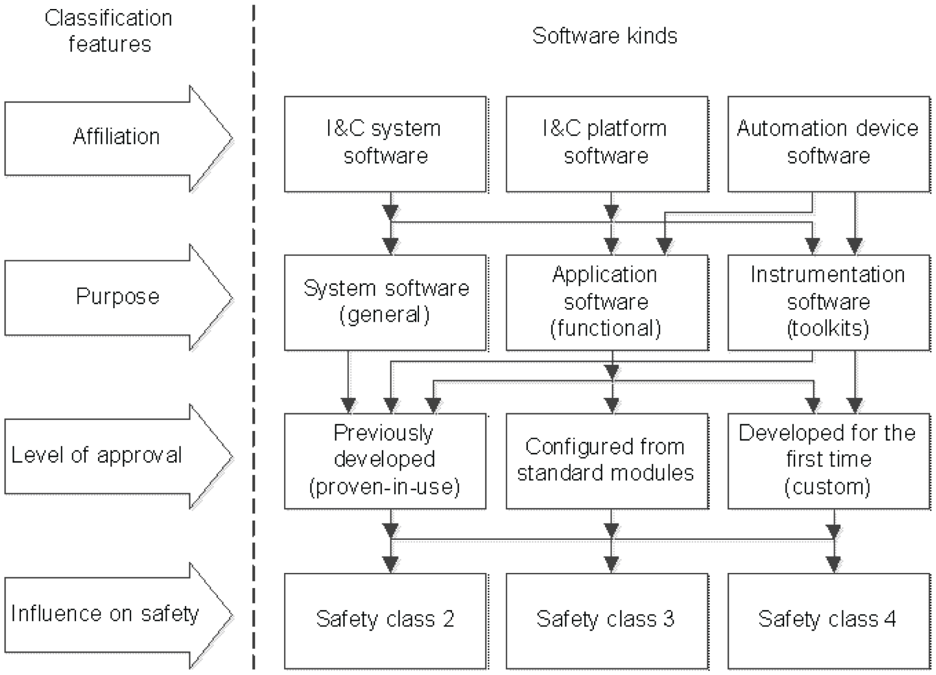
7. Nuclear power plant I&C systems are complex systems which can consist of several subsystems, each produced with the use of one or several platforms. Consequently, software of I&C system is a set of various software components (computer programs), which differ in functional purpose, developer companies, programming languages and technologies used, etc. This causes asymmetry of requirements for different software components.
8. Quantitative requirements for reliability are difficult to establish for software, in contrast to I&C system hardware items. There are several factors causing the absence of common and standard methods of quantitative evaluation of software reliability. These factors include: uniqueness of software as an object of evaluation, in spite of actively continuing industrialization of development processes and introduction of numerous standards for techniques of developing software; insufficient development of theoretical aspects of this evaluation and lack of a mutual opinion about its expediency; complexity of representing objective and complete information on defects that are discovered at different stages of the software lifecycle, and others.

Classification of I&C Software

Specification of requirements for different kinds of software depends on and usually based on I&C software classification. The following classification features are recommended to use (see Figure 1):

- Affiliation of the software with various I&C system and subsystems.
- Functional purpose.
- Level of approval.
- Effect on safety.

Figure 1. Classification of I&C software


Classification features
Software kinds
Affiliation
Purpose
Level of approval
Influence on safety
I&C system software
I&C platform software
Automation device software
System software (general)
Application software (functional)
Instrumentation software (toolkits)
Previously developed (proven-in-use)
Configured from standard modules
Developed for the first time (custom)
Safety class 2
Safety class 3
Safety class 4

The selection of these classification features is made on the basis of analyzing modern international standards for I&C software, which are important for nuclear power plant safety, in particular (IAEA, 2000), (IEC, 2006, a) and (IEC, 2008).

Based on these features software has a multidimensional (parallel) classification, in which individual groups of its types are relatively independent. The arrows between components of individual facets indicated the most preferred combinations of software types, which are classified according to different features. It should be noted that some facets can be more detailed and presented in the form of hierarchical classifications.

By affiliation software can be a part of: I&C system, I&C platform, some automation devices or equipment.

Based on purpose software is classified into: general (or system) software; application (or functional) software; instrumentation (or toolkit) software, which is used in development, testing and verification. The examples of instrumentation software include different tools, which are intended for processes of design, translation, configuration control, debugging, and verification.

Level of approval is an important classification feature according to which there are:

- Previously developed (proven-in-use) software, also known as off-the-shelf (OTS) software. This kind of software can include commercially accessible software, developed and supplied by other companies, and also standard application software, which is created and approved in similar or different projects.
- Software configured from standard (previously developed) software modules (library blocks). The configuration tools for such software usually is proven-in-use software.
- First time developed (custom) software. Such software is created especially for the given system and has no operational experience in other applications.

Previously developed (OTS) software further be classified by other features, such as source code availability (openness), possibility of changes, amount of operating experience, etc.

Influence on safety is determined by I&C system safety class in which this software is used. According to the Ukrainian legislation any I&C system must be assigned to one of three safety classes, denoted by numbers 2, 3 and 4. Moreover for functions performed by I&C system are assigned to the category denoted by letters A, B or C. Therefore I&C system can be:

- Safety class 2(A), if at least one function of that system has category A.
- Safety class 3(B), if system does not perform category A functions and at least one function of that system has category B.
- Safety class 3(C), if system does not perform category A and B functions and at least one function of that system has category C.
- Safety class 4, if none of its functions are classified by category (such systems are consider as non-safety).

It is important, that affiliation of software does not affect I&C software requirement directly. Purpose of software affect on the requirement, because special set of requirements is established for tools that are used for development and verification. Level of approval strongly influences the software requirements, e.g. required methods and scope of verification can be very different for proven-in-use and for custom software. But, of course, the greatest dependence is between software requirements and influence on safety, expressed by Safety Class. Moreover, safety class defined for I&C system imposes requirements for software of all components, platforms and even related automation devices.

The Criteria of Selection and Structuring of Requirements

Selection and any activities aimed at meeting requirements are impossible without establishing a clear classification features, determining factors and selection criteria. The main factors and criteria are considered below.

1. General criteria for selection of requirements or, in other words, "requirements for requirements." Among such criteria for nuclear power plant I&C software the most important are the criteria of necessity, completeness, adequacy, correctness, verifiability, and openness. These criteria are related to the criteria that were developed and are used for evaluating the execution of requirements for software during expert analyses (Vilkomir, 1999), (Vilkomir, 2000). For example, in accordance with the criterion of completeness during generation of many requirements for software elements must be separated and taken into account that reflect "covering" by requirements of these components such as: completeness of conformity to specifications; completeness of consideration of software lifecycle stages; completeness of the diagnostics, and so forth.
2. Classification and content of I&C system requirements as a whole. The full set of these requirements includes:
   a. Requirements for the composition of the functions.
   b. Requirements for quality of the execution of these functions.
   c. Requirements for reliability of function execution.
   d. Requirements for stability of function execution against external influences.
   e. Requirements for lack of influence on other systems.
   f. Requirements for procedures and processes that support meeting requirements for functions, quality, reliability and stability.

This set should be designed for the full set of software requirements and should be correspondingly supplemented and specified. In particular, the subsets of requirements for processes of software development and verification, which play a priority role from the standpoint of assurance of reliability and safety, should be expanded and worked out in maximum degree.

3. Particular features of software as an object of safety standardization. The following set of the software features have a direct effect on the selection of classification features and generation of subsets of requirements:
   a. Software is both a component of the system for which regulatory requirements have been established and a means that assures fulfillment of the regulatory requirements for I&C system. Consideration of this feature is most important in defining requirements for monitoring and diagnosis, reliability and stability. In doing so different external disturbing influences for software should be examined.
   b. Software is a possible source of common cause failure. Nature of software makes it necessary to have requirements for protection from common cause failures due to improvement of software development and verification processes and use of the diversity principle, which in turn determines the necessity of classification features

for methods and means of diversity implementation.

c. Software is a multi-component system. During the statement and classification of requirements the purpose, level of approval and safety class of different software components have to be considered.

d. Software is a product and a process. This feature of software is one of the critical ones in selecting classification features of requirements and generation of their complete sets, which considers the certain influence of development and verification processes on software characteristics.

4. The existing regulations, which include standards determining software requirements. On the basis of these standards requirements for I&C software can be selected as the so-called normative profile for software. In the general case normative profile is a subset and/or combinations of the positions of basic standards for a specific subject area, which are required for implementation of the required functions in the system. In this case, we mean the normative profile of requirements for I&C software that is important for nuclear power plant safety. The said standards form the profile-forming base for producing the normative profile of software requirements (for example, software lifecycle models, structure of requirements for software, set of metrics and methods of evaluation, requirements for tools, etc.).

5. Possible variants of requirement structuring. This factor is conceptual in nature, because it determines the general approaches, priority and interconnection between different requirements for I&C software. Several variants of software requirements structuring are possible:

   a. Product-oriented: requirements that determine characteristics for software as a component of I&C system. It does not take into account the fact that software characteristics are built in and implemented at different stages of the software lifecycle.

   b. Process-oriented: requirements correspond to software lifecycle processes and define features of process and intermediate product of each stage in the form of "stage-tasks-requirements" statements. This approach is widely used and allows clear process management and quality assurance, but complicates the definition of software product features and for complex software can lead to difficulties with integration.

   c. Mixed process-product-oriented: requirement are divided in two groups and describe both features of development processes and features of final product. In this case the advantages of the first two approaches are used.

General and Functional Requirements

The classification of software requirements can be performed in two stages: in the first stage, which corresponds to the upper level of the hierarchy, we determine the place of normative requirements among the full set of requirements for software (classification of kinds of requirements for software); in the second stage, which corresponds to the lower level of the hierarchy, we carry out the classification of general requirements for software, based on the process-product approach.

The set of requirements for software corresponds to the set of requirements for I&C system, because it contains both requirements and functions, and for their quality (properties), and to reliability, stability, and processes (both development and verification). The particular features of this full set for software consist of:

1. Requirements for software as an element of I&C system are determined based on requirements for the I&C system as a whole.
2. Requirements for the structure in software elements precede requirements for functions. In this case we are speaking of general requirements for software functions that are important for safety, and not about functions that are determined by its purpose.
3. Full set of quality characteristics we have separated out one, which is most important from the standpoint of safety standardization, which determines the requirements for monitoring and diagnostics.
4. Requirements for processes are determining to a great extent, because they are expanded and worked out in detail with consideration of safety assurance.

In order to conduct classification for requirements we shall distinguish three features: source of requirements; type of requirements; object of requirements assignment (Figure 2).

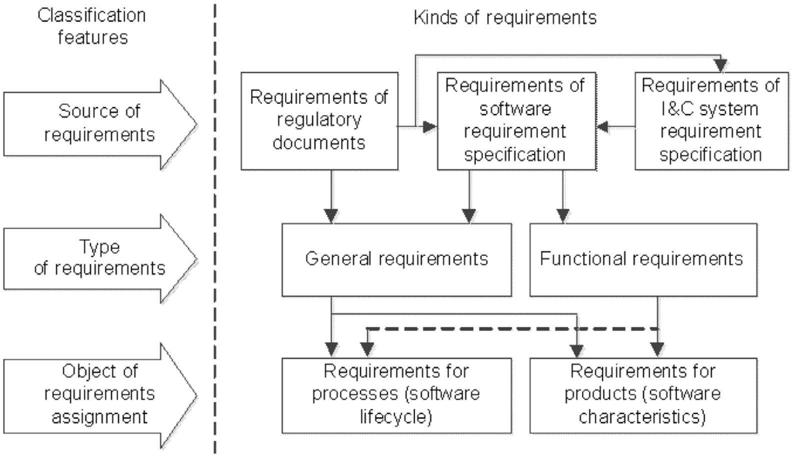
For the first of them we can distinguish requirements of the regulatory (normative) documents and requirements that are contained in the requirement specifications for development of I&C system and development of software.

In the development of specifications for software or I&C system (as a whole) requirements of the regulatory documents must be taken into account. Requirements of the specifications of the software are developed with consideration of the specifications for I&C system.

According to the type of requirement software requirements are divided into general and functional. General requirements do not depend directly on what the functions are implemented in I&C software, but are determined only by the safety class, level of approval and its purpose. Functional requirements depend completely on the purpose of the I&C and tasks which are solved by the software. The functional category normally includes requirements for productivity, synchronization, information protection, required service lives, portability and so forth.

Depending on the object of assignment one can distinguish requirements for software lifecycle processes (development and verification) and product requirements (software characteristics). In the regulatory documents general requirements

Figure 2. Classification of software requirements


Classification features
Kinds of requirements
Source of requirements
Type of requirements
Object of requirements assignment
Requirements of regulatory documents
Requirements of software requirement specification
Requirements of I&C system requirement specification
General requirements
Functional requirements
Requirements for processes (software lifecycle)
Requirements for products (software characteristics)

are normally given as those pertain to processes and products. Functional requirements as a rule pertain to software and to the product, although they can determine some of the requirements for the process of software creation with consideration of specific features of the design, the tools used and so forth.

Below we examine the classification and perform an analysis of the general requirements.

Results of the classification of general requirements for software characteristics (software as a product) and processes of its creation are given in Figures 3 and 4 respectively. In the classification of requirements for software characteristics two groups of requirements are delineated: for structure and for properties. The first group includes requirements for features of the construction and functioning of software. The second of these groups brings together requirements for software properties such as requirements for its sufficiency and adequacy for functions execution, monitoring and diagnosis, reliability and stability.

Requirements for Software Characteristics

Requirements for structure and components includes the following requirements:

1. Requirements to modularity.
2. Requirements to use of off-the-shelf components (pre-developed software).
3. Requirements to interfaces.
4. Restrictions for use of the operating system and interrupts.

The first subgroup of the requirements is due to the need to present software in the form of a modular structure. In doing so the source code of one module must contain a limited number of operators, and the modules must have a clear structure, be easily modifiable and tested.

The second subgroup determines the preference of the use of previously developed software. Using OTS software components one must: evaluate its conformity to the functions and characteristics of I&C system, where the use of OTS components is preferred for which one should determine the functions and characteristics of the OTS components and correlate them with specifications for I&C software; analyze the results of OTS components operation from the standpoint of its conformity to the adopted criteria, norms and rules of safety; develop, if necessary, a list of the required modifications for adaptation of the OTS components to conditions of its use in I&C system; execute such adaptation and perform testing; develop and

Figure 3. Classification of requirements for products (software characteristics)

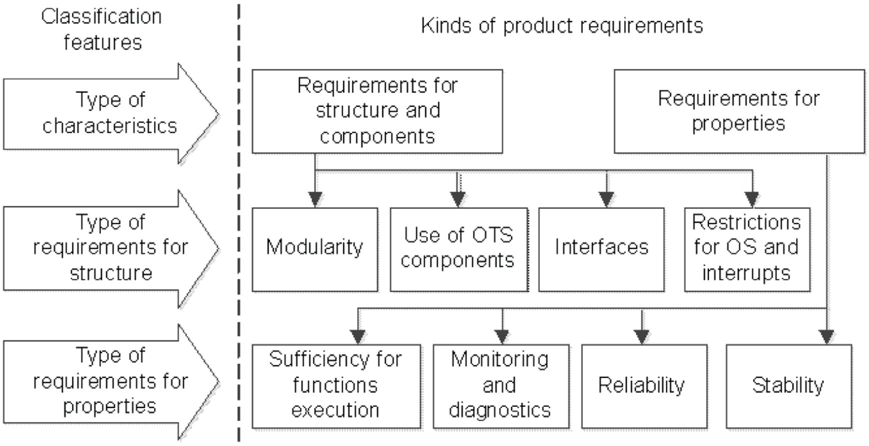
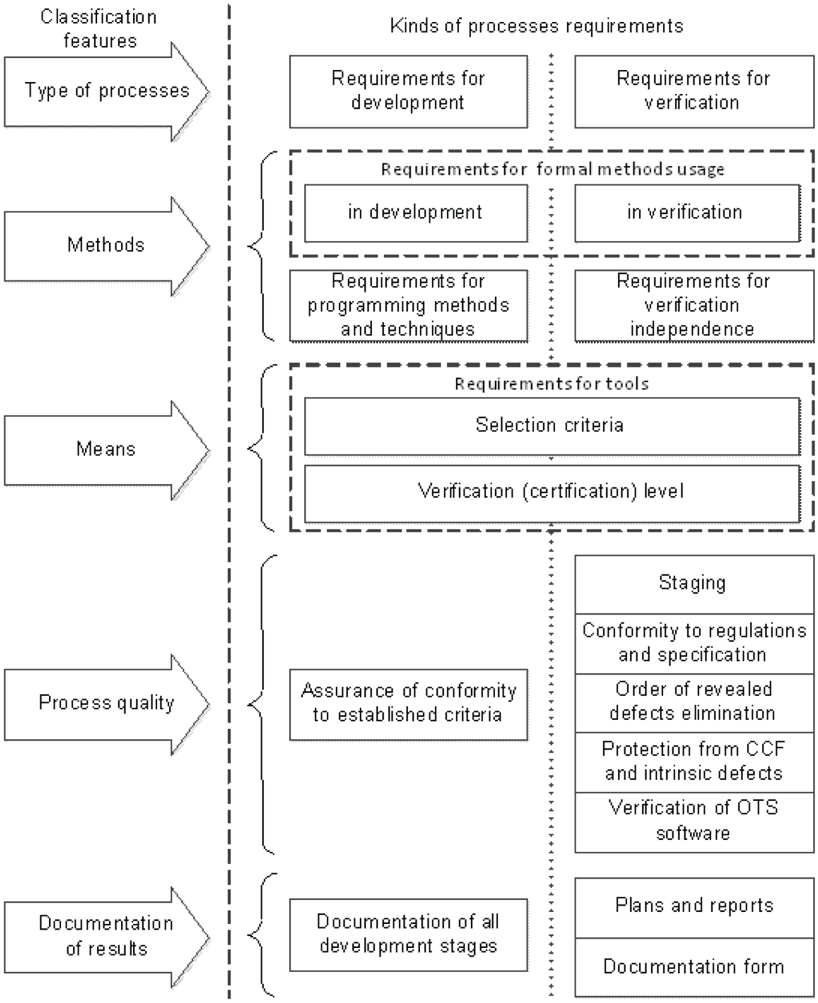

Classification features
Kinds of product requirements
Type of characteristics
Requirements for structure and components
Requirements for properties
Type of requirements for structure
Modularity
Use of OTS components
Interfaces
Restrictions for OS and interrupts
Type of requirements for properties
Sufficiency for functions execution
Monitoring and diagnostics
Reliability
Stability

Figure 4. Classification for requirements for processes (software lifecycle)


Classification features
Kinds of processes requirements
Type of processes
Requirements for development
Requirements for verification
Methods
Requirements for formal methods usage
in development
in verification
Requirements for programming methods and techniques
Requirements for verification independence
Means
Requirements for tools
Selection criteria
Verification (certification) level
Process quality
Assurance of conformity to established criteria
Staging
Conformity to regulations and specification
Order of revealed defects elimination
Protection from CCF and intrinsic defects
Verification of OTS software
Documentation of results
Documentation of all development stages
Plans and reports
Documentation form

implement the plan for verification of the changes made. The amount and extent of evaluation of conformity of OTS software components to these criteria are determined by the safety class (I&C safety class). The importance of requirements for the use of OTS components (both developed as special purpose and COTS-components) for safety of the I&C systems as a whole should be emphasized. According to existing estimates (Kersken, 2001), the amount of OST components in software of mature systems can reach 80-85% of the total amount of software.

The third of the listed subgroups of requirements determines the need for complete and clear description of the interfaces between the software being examined and the operator (also known as human-machine interface), hardware platform and peripheral hardware (sensors, drives and so forth) of a given I&C system, and also other I&C devices, systems and subsystems. This description determines the limits of the software being analyzed.

Restrictions for use of the operating system and interrupts are included in requirements for I&C software of safety class 2. If the use of the operating system is deemed necessary, it should execute only the simplest functions. The use of interrupts in the course of executing the most critical functions should be prohibited. One should note that in order to fulfill this requirement more precise criteria should be developed, after providing a detailed explanation of the functions for which the use of the operating system must be limited.

Requirements for monitoring and diagnostics can be divided into four groups with consideration of the kinds of processes and objects, for evaluation of the state of which software is used:

1. Requirements to monitoring I&C system by programming means.
2. Requirements to diagnosis (search for malfunctions) of I&C system by software means.
3. Requirements to self-monitoring of software.
4. Requirements to self-diagnostics of software.

In other words the main requirements for monitoring and diagnosis are:

a. Software should perform (a) continuous automatic monitoring of operating condition and (b) periodic function checks of the I&C system.
b. Software should provide diagnostics of I&C system at the level required by specification.
c. Software should provide self-monitoring and self-diagnosis.

For this purpose, the following should be used: monitoring of intermediate and the final results of the execution of programs and their allowable duration; repeated counting and comparison of the results; discovery of prohibited situations; monitoring data in memory and so forth. For monitoring of I&C software of safety class 2 different types of diversity can be used.

It is necessary that in the process of monitoring and diagnosis: all functions are checked that are important for I&C system safety; during periodic testing it is mandatory to check devices which are not built-in or permanently connected monitoring devices; all degradations of characteristics of safety functions are discovered on a timely basis; if any failure is discovered timely automatic actions that correspond to the situation are generated.

Moreover, an important part of requirements for monitoring and diagnosis are the requirements related to execution of mandatory limitations and procedures during their implementation: implementation of monitoring and diagnostic programs (self-monitoring and self-diagnostics) should not affect fulfillment of programs of the main information and control functions and/or lead to unacceptable degradation of a characteristic; one should make an analysis of the situations and procedure, which allow to avoid false errors; the software should provide automatic recording, storage and display of data on results of monitoring and diagnostics (self-monitoring and self-diagnostics).

Requirements for reliability and stability: By reliability of software we mean its property of preserving serviceability and converting raw data to the result being sought under the given conditions in the assigned time. By stability of software we mean its ability to execute its functions in anomalous situations (during breakdowns and failures of hardware devices, operator errors and errors in the raw data) (DSTU, 1994).

Requirements for software related to assurance of reliability and stability can be classified according to a scheme, whose basic elements are: sources of failures and influences on software and I&C system; kind of failures and influences; methods of protection from them.

Sources of failures can be: internal sources with respect to I&C system (both software and hardware); external sources with respect to the I&C system (other I&C systems; operating personnel; repair personnel).

By kind of failures, which should be compensated by means of programming devices, we can distinguish: failures (breakdowns) of hardware devices; failures (breakdowns) caused by the appearance of software defects, which are introduced at the design stage and are not detected during testing and verification.

In turn, software anomalies that can be the cause of I&C system failure are classified into:

1. Defects that appear under certain conditions of the system, its individual components and sets of input signals.
2. Defects that appear during non-standard functioning of hardware of the I&C system.
3. Defects caused by incorrect or incomplete specifications of the software.
4. Defects introduced in development of the software (at all stages of the lifecycle).
5. Defects related to the use of tools and that depend on other software and interfaces between parts of the software or other systems.

The main kinds of influences, resistance to which should be assured by software are the following: unintentional or intentional errors of personnel; unauthorized actions or unauthorized access to programs, data, operating systems; malicious software, including viruses, spyware and trojans, which are sets of instructions that execute actions not stipulated by the specifications and that represent a threat to safety; distortions of incoming information that arise from measurement devices (sensors) and along communication channels from other systems.

Thus, requirements for software related to reliability and stability consist in that the software must implement protection from all of the listed kinds of failures and actions. In this case protection should be assured from failures by general factors, which are due to the appearance of intrinsic defects of the software, by failures and breakdowns of hardware devices of the I&C system.

Protection against failures: The following methods are used to protect from the listed kinds of failures and influences on software.

1. Technical diagnostics (monitoring and determination of the cause of a failure or breakdown), reconfiguration of the structure and restoration of the computational process or control process. This method is universal and by appropriate loading of its constituents can assure protection from a broad class of failures. In the I&C system it should be used for protection from hardware failures.
2. Software, functional or other kinds of diversity. The use of diversity is a systems requirement, which is aimed at protection from common cause failures and is related to the use of different kinds of redundancy in the process of creation (development and verification) of software and in the final product, i.e. the software itself. Software diversity (usage different software versions) is achieved by using different algorithms, languages, libraries, programming approaches, operating systems and so forth. Functional diversity is assured by using more than one criterion for identification of each situation that requires the initiation of control actions.

It should be emphasized that for software of safety control systems, which execute emergency protection functions, the emergency situations must be discovered by several methods based on different physically interconnected production parameters, while the analysis of data on the values of these parameters should be performed by different software modules.

For I&C software of safety class 2, in addition, when using software, functional or other kinds of diversity, one must: evaluate the degree of correlation of different versions (analyze the actual level of diversity), their capability for joint compensation of software defects; analyze the substantiation and influence on safety for additionally introduced components - different software or hardware versions. Software diversity should not create a danger of non-fulfillment of functional requirements.

3. Establishment of access categories, application of different password systems, digital signature procedures, use of special encoding algorithms and others. These methods assure protection from errors of personnel and unauthorized actions.
4. Monitoring reliability and protection of incoming information from distortions. In this case one should check: incoming signals being present in zones of access, established in accordance with the specification; logical non-contradictory nature of values of input variables and so forth.

Note that during the use of all protection methods software is an object of protection and a means of assuring reliability and safety. In this case, there must be the introduction of additional software components, which in turn can be sources of failures and therefore they must be carefully analyzed. Functional characteristics of the software and I&C system as a whole should not be degraded to an unacceptable value (just as during monitoring and diagnostics).

Protection against cyber threats: The software of I&C system shall be protected from undesirable and unsafe interference to work and unauthorized changes via external computer networks and the use of non-resident storage media.

To achieve such protection connection with Internet shall be excluded and any changed can be possible only after appropriate authorization. Also special methods of protection from viruses and other malware should be used.

At the same time, measures against cyber threats should not affect the execution of applications software and deteriorate performance of the functions that are implemented by software.

Requirements for Development of Software

Requirements for methods of software development are divided into two main groups:

1. Requirements to use of formal methods.
2. Requirements to programming methods and approaches.

The first group of requirements is to a certain extent recommendatory in nature and indicates the need (expediency) of using at all stages of development and verification formal methods that are based on rigorous mathematical description of formulations of problems related to different stages of software improvement and verification with use of a theoretical apparatus of algorithms, mathematical logic, graph theory and so forth, and also on proof of the correctness of solving these problems by means of standard procedures. Such methods are used in particular for:

1. Transition from verbal to formal description of general and functional requirements for software and development of its formal specifications.
2. Mathematical proof of the conformity of software to specifications or requirements of previous stages of development.
3. Development of application programs using formal procedures of synthesis.
4. Analysis of syntactic and semantic correctness and carrying out test verifications of execution of functional requirements for software.
5. Improvement of the verifiability of software and formalization of the evaluation of results during independent verification and validation.

The best developed and best known methods of formalized checks of software are methods based on formal procedures of logical output, proof of the correctness of algorithms and programs (Anderson, 1979), and also FTA- and FME(C)A-analysis methods that are widely used to analyze hardware (IEC, 2006, c) and (IEC, 2006, b). The first of them is based on constructing fault tree and events analyses. The second is based on analysis of the fault modes and effects criticality analyses.

The second group of requirements is determined by the preference of using standardized designations of variables in software, files of constant and predefined length, subroutines with minimal number of parameters (e.g. with one output and one input), etc. Moreover, this group of requirements is related to the need to exclude methods in programming development that complicate the software, e.g. complex branches and cycles in the programs, complex indexes in the files and so forth. Note that in the methodological normative documents, which are used in some countries, requirements are contained regarding the need of use of systems in software development that are important for nuclear power plant safety, special methods that improve its reliability, in particular the so-called method of defensive programming (Lawrence, 2002), (Ben-Ari, 2000).

Requirements for tools used to develop software reflect two aspects that are related to their usage:

1. Determination of the criteria for selecting automated development and verification tools.
2. Degree of verification of these tools.

It should be noted, that in the existing normative documents the selection criteria of tools are not given, but the need for the software developer to provide substantiation of such criteria and demonstrate proof that the devices used conform to them is postulated.

The main principle applicable for the tools is that tools used to generate code, must pass through verification with the same requirements as the I&C software itself.

Requirements for Software Verification

Software verification is an important part of I&C software lifecycle. Verification of software is defined as the process of proving the conformity of results obtained at a certain stage of software development with the requirements established in the preceding stage. As noted earlier, the majority of requirements for methods and means of development and verification are uniform. An important distinguishing feature of this group of requirements for verification is the necessity of assuring its independence, that is, carrying it out by persons who are not direct developers of the software.

Requirements for verification independence: The integral requirements of independence are level of independence of the experts (organizations) that conduct software verification, and the agreement of these levels with the software safety classes.

The following levels of independence are possible:

1. **Maximum Independence:** Verification is conducted by experts or organizations that administratively and/or financially are independent of the software developers. This level of independence can be broken down into two sublevels:
   a. Administrative independence.
   b. Administrative and financial independence. In this case we are speaking of conducting verification by representatives of a different organization, which specializes in solving such tasks.

2. **Partial Independence:** Verification is carried out by other experts of the same organization, and their administrative and/or financial independence from the software developers is not required. In this case there can be partial administrative and/or financial independence, if the verification is conducted by experts of a different subdivision of the organization, for example by representatives of quality control service, are subordinate directly to the director.
3. **Minimal Independence:** Verification is conducted by the developers themselves, and the review of its results is performed by other experts.

By means of the technology of independent verification and validation (IV&V) one can implement the principle of diversity with respect to the software creation process. In order to assure the highest degree of verification it is necessary that one use tools (utilities), that are different from those which the developer used.

It should be noted that conducting an independent verification can be accomplished according to different systems and with different depth, which depends on the software safety class, worthwhile tasks and existing resources.

Actually three basic scenarios of verification implementation are possible:

1. Full verification and validation of the entire project is carried out, which repeats practically all stages of verification within limits of the project, using intrinsic (diverse) tools and methodologies.
2. Independent consecutive evaluation (rechecking) of all results of the verification performed by the developer organization is carried out. In this case all checks are conducted that are stipulated by the verification and validation plans, and also checks proposed by specialists of the expert analysis organization, and tools of both the inspected and inspecting organizations are used.
3. Independent sampling evaluation (recheck) of results of the verification of the most important functions from the safety standpoint is carried out, which is made by the developer organization.

Quality of verification: The use of independent verification and validation techniques allows one to improve the quality of this process. By software verification quality we can mean the degree of conformity of software to regulatory requirements after it is carried out and elimination of any discovered defects.

The verification quality is evaluated by analyzing fulfillment of the following requirements:

1. Requirements to staging of the process. The essence of the requirement consists in that the verification must be carried out after each software development stage (specification, design, and coding and others).
2. Requirements to verification of software conformity to requirements of normative documents (general requirements for characteristics and software development, described earlier) and specifications (functional requirements).
3. Requirements to order of elimination of any discovered defects and malfunctions. Components of this requirement are constituents of the process of elimination of defects, time periods for defect elimination, conformity of the time periods of elimination of defects to the software safety class. The process of eliminating defects, independent of the software safety class, includes that a mandatory stabilizing when discovered in the process of development, testing and verification; analysis of the causes, degree

of influence on safety; introduction of the necessary changes to the software; repeated check of software with documentation of the results.

4. Requirements to protection from intrinsic defects and common cause failures. Elements of this check are discovery of potential sources of CCF, caused by defects of the software or other components; analysis of their influence on safety of the software and I&C systems as a whole; evaluation of the effectiveness of using devices to protect against these failures.
5. Verification of different kinds of software, including previously developed (OTS) software.

Requirements for documentation: Documenting is an important part of the verification process and implies the development of two basic documents (groups of documents):

1. The software verification plan, which can consist of a general (coordination) and several particular verification plans and test methods;
2. The software verification report (reports and test protocols) for software verification.

Requirements for documenting software verification results include requirements for the presence, structure and content of a plan (plans), produced before the beginning of verification, and report (reports), which is produced based on results of verification and requirements for the form of material presentation.

All documentation related to development and verification should be set forth in an accessible form, understood by experts, who did not participate in creating the software. The given requirements imply, in particular, traceability of all actions executed in the verification process, which allows one to establish a comparison between the input and output elements at each of the software creation stages and to make a transparent check of the completeness of execution of all requirements, beginning from requirements for the I&C system, then general and functional requirements for the software and ending in reports on verification (tests) of different subsystems or software functions.

The software verification plan should determine: choice of verification strategy and sequence for conducting it; methods and devices used in the verification; sequence of documenting actions and evaluation of verification results.

EVALUATION OF SOFTWARE FOR NUCLEAR POWER PLANT I&C SYSTEM

Criteria and Principles of Evaluation

The goal of the software evaluation is to check conformity to established requirements. This evaluation is conducted by analyzing the documentation submitted by the software developers, and also by verification of software using special tools. The project documentation (for example, the design description) and documents issued by the developer particularly for the licensing purposes (for example, safety analysis report) can be examined. During the expert evaluation some additional information can be requested from developer to clarify issues of the main documentation.

The purpose of the expert work is to improve the level of quality and reliability of the software. Therefore, all comments and recommendations of the experts should be transferred to the developers for timely elimination of any discovered defects. As a result of the joint activity of developers and experts corrections can be made to the design and, thereby, reduce the number of software defects.

The basis of the software expert evaluation methodology is assessment of the meeting the requirements for software at different stages of the lifecycle. In this case it is necessary to evaluate functional and general requirements for software, and also requirements for development and verification. The indicated requirements are to be combined in the criteria, which the software must satisfy, as well as processes of development and verification.

It is suggested that the following five criteria be used (Vilkomir, 1999):

- Completeness
- Documentation
- Accessibility
- Independence
- Successfulness

Software meets the criterion of completeness if its specifications completely correspond to the specifications of the I&C system and the software meets general and functional requirements of the specification, including requirements for development and verification.

Software meets the criterion of documentation, if the composition and structure of the documents developed for all stages of design, verification and operation, correspond to requirements of standards, norms and rules. The documentation criteria and completeness are interconnected: in accordance with the completeness criterion the content aspect of software development is analyzed; in accordance with the documentation criterion the formal aspect of evaluation is evaluated.

Software meets the criterion of accessibility if the documentation for development and verification of software is presented in a form that is clear and understandable to experts, who do not participate directly in their development. Moreover, in accordance with this criterion traceability (transparency, verifiability, checkability) of step by step execution of requirements for software at different stages of the lifecycle must be assured.

Software meets the criterion of independence if the degree of independence of software checking corresponds to the safety class of the system. For systems of safety class 2 the evaluation must be performed by a group of experts (organization), which is administratively and/or materially independent of the experts (organizations) which developed the software. For systems of safety class 3 the development and verification must be carried out by different specialists, however the administrative and financial independence is not required.

Software satisfies the criterion of successfulness if the inspection was successfully completed before beginning of system usage and if by that time all discovered defects and deficiencies have been analyzed and eliminated.

The criteria are an important part of the overall system of software evaluation. Conformity of the criteria and evaluated requirements can be given in the form of a matrix, which contains particular evaluations of the meeting individual requirements and summary evaluations based on the criteria. At the outset the evaluation in accordance with each of the five previously described criteria is formed on the basis of analyzing individual requirements, and then a concluding evaluation is produced.

Along with the general principles of systems approach and expert knowledge additional principles shall be implemented in the expert evaluation of software:

1. The principle of diversity of methods, hardware, actions of experts, methods of generating expert evaluations of software. This requirement determines the internal diversity of the evaluation process, thereby supplementing external diversity, which results in the fact that the expert evaluation and independent verification assure increasing reliability of software evaluation.
2. The principle of asymmetry of efforts distribution. A particular feature of software evaluation is the fact that due to its complexity it is impossible to assure complete testing of the behavior of software for all theoretically possible sets of input data. Therefore,

while carrying out expert evaluations under conditions of limited time and resources the main efforts must be concentrated in critical steps and results of software development, analysis of the completeness and reliability of tests.

Next we will propose the content of operations for software evaluation at all basic stages of the lifecycle: development of requirements for software, design and coding of software, verification (development of the verification plan, preparation of the verification report).

In the stage of software requirements development the evaluation contains three steps: evaluation of the conformity of requirements for software to the requirements for the system; evaluation of the representation and specifications of requirements for software and general requirements; transfer of findings to the developer and obtaining back the corrective and additional requirements.

At the software design stage the evaluation contains four steps: evaluation of implementation of software requirements in the design; analysis of the structure for a subject of assured protection from common cause failures due to software errors; listing of requirements and functions of software for use in subsequent stages of the evaluation; transfer of findings to the developer and obtaining from him information and corrective actions for software design and evaluation of their adequacy.

At the stage of software verification plan development the evaluation contains four steps: evaluation of the existence in the verification plan of programs and methods for software testing; evaluation of accessibility of the verification plan; evaluation of reflection in the verification plan the requirements from the detailed list, which is compiled in the preceding stage of the evaluation; evaluation of the completeness and adequacy of the number of tests included in the verification plan. If necessary these stages can be supplemented by defining recommendations for additional testing of the functions more important for safety, transmission of comments and additions to the developer and obtaining a corrected and supplemented verification plan from him.

In the stage of software verification report preparation the evaluation contains six steps: evaluation of the existence in the verification report of protocols and official statements for each program and method of testing; evaluation of the completeness of the tests carried out; evaluation of independence of the verification conducted; evaluation of the software tools used in the development and verification; evaluation of the rate of success of completion of all tests; statement of recommendations for the regulatory body on the possibility of using the software.

The stages of evaluating the plan and the report on software verification are the most important. At these stages the regulatory body has the opportunity to receive evidence of achievement of the required level of quality and reliability of the software. For this purpose the plans, programs and methods of software testing are evaluated before the beginning of the tests, and the additions and comments made are transmitted to the software developer for their consideration.

Evaluation of Software Characteristic

Tasks and approaches to evaluation: Evaluation of the software characteristics includes the following tasks.

The first task is analysis of software conformity to general requirements defined in national and international standards. These requirements do not depend directly on the functional purpose of the software, but are determined by the designation and safety classification of systems.

The second task is evaluation of the completeness and quality of implementation of functional requirements in the software, which are defined in the software requirement specification. For reusable software an evaluation of the conformity of functions implemented in the software to the requirements is determined based on the context of the intended usage.

The first of the listed tasks is universal in nature and therefore can be partially or completely formalized. To this end, general methodology should be defined. Such methodology can include: obtaining the normative profiles (requirements) of the software; development (systematization, profiling, selection) of parameters for evaluation of characteristics (properties) of software and the established requirements; analysis of the results of evaluation and determination of the level of satisfaction of the requirements established for software; procedures (algorithms) of software evaluation using different parameters.

The evaluation of software requires determination of the composition of the corresponding characteristics and parameters, and also methods of their evaluation. Software quality can be evaluated by several characteristics, among which there are functionality, reliability, usability and so forth. The significance of each of these characteristics depends on the area of software application. For software systems that are important to safety a determining characteristic is reliability.

Given the controversies regarding the understanding and use of the term "software reliability" two existing approaches to its evaluation, which conventionally are called "qualitative" and "quantitative," can be considered.

The qualitative approach is used everywhere and is oriented to a system (hierarchy) of requirements, i.e. profiles determined by standards, industry regulations and normative documents of companies, the fulfillment of which is checked during software reliability evaluation. Results of reliability evaluation in this case are formulated in the form of the conclusions "corresponds" or "does not correspond" for individual components, which directly or indirectly affect reliability.

The quantitative approach to evaluation is oriented to the development of models, that receive as input parameters characteristics of both processes (development and verification) and software itself, and gives as output the indicators that characterize reliability (Lyu, 1996).

These indicators most frequently are analogues of reliability indicators of equipment with the difference that such events as "component failures," are formulated as "manifestation of software defects." Moreover, special indicators (metrics) are also used that determine the level of residual defects, rate of their discovery during testing and so forth.

Nevertheless, the instability of the manifestation of defects in sophisticated software systems and their uniqueness do not allow one with high degree of accuracy to determine quantitative values of the characteristics of quality and reliability. To solve this problem, the special methods of analysis such as FTA (Fault Tree Analysis), RBD (Reliability Block Diagram), FME(C)A (Failure Modes, Effects (and Criticality) Analysis) and others, can be used.

Metrics, indicators and raw data for evaluation: There are different approaches to defining of metrics and their relationship to the concepts of software quality and reliability indicators (Pressman, 1997).

The first approach (in accordance with the IEEE standards (IEEE, 1990), (IEEE, 1988, a) and (Pressman, 1997)) views this relationship on the basis of the categories "absolute-relative" and is based on the following definitions.

Absolute indicators (measures) are quantitative indicators that characterize absolute values of different attributes of software and the development process (for example, the number of defects discovered in each software module, the number of lines of initial software text and so forth). In this approach the metrics, in contrast to absolute indicators, are intended especially for comparison of different software designs. For example, comparison of two software applications based on an absolute indicator such as total number of defects discovered is not informative because lack of possibility for judging the size (measured in the lines of source code or number of operators) of comparable programs, their complexity, conditions of development, testing and other characteristics. It is obvious that it is more expedient in this example to use metrics that determine the relationship of the total number of defects to the size of software, quality of programming modules, test time and so forth.

The special feature of the second approach is the fact that metrics are interpreted as dedicated indicators (supplemental with respect to known indicators), which can be given as absolute or relative evaluations of software.

It should be emphasized that the boundary between metrics and reliability indicators of software is quite difficult to draw. Reliability indicators are primarily quantitative characteristics similar to indicators used in classic reliability theory (probability of no-failure, mean time before failure and so on), while metrics are specific indicators for software, which can evaluate reliability indirectly or with respect to other products (reference standards).

Next we will discuss metrics with consideration of the more common second approach. It should be noted that metrics can also give a quantitative evaluation of any given property as well as requirements for software. In this case, by raw data, or parameters (primitives) of metrics we mean the initial quantitative values that are needed for their calculation. The raw data can be other indicators or metrics as well as different constants, coefficients and so forth.

Software developer organizations should be encouraged to use various metrics, because they allow one to evaluate the level of quality and reliability of software being developed and their design processes, and also to discover existing problems (for example, inadequate testing of software, failure to follow the standards, ineffective work of individual groups of developers and so forth) and to take the necessary measures to solve them. Moreover, the need for calculation and analysis of various metrics arises during verification and validation of software, because these processes must rely to a greater degree on accurate quantitative evaluations, and not on subjective opinion of developers or customers.

Basic standards that define metrics and sequence of their computing are:

- IEEE standard 982.1-1988 (IEEE, 1988, a), which defines the list and order of reliability metric calculations.
- IEEE standard 982.2-1988 (IEEE, 1988, b), which clarifies the sequence of using the standard IEEE 982.1-1988.
- ISO/IEC standard 9126-1:1999 (ISO, 1999), which defines the software quality model.
- Technical report ISO/TEC TR 9126-2:2000 (ISO, 2000), which establishes the basic nomenclature of external software quality metrics, including metrics of reliability, and defines basic principles of their selection and evaluation.
- Ukrainian standard DSTU 2850-94 (DSTU, 1994), which repeats the basic principles of the international standard ISO/IEC 9126 (ISO, 1999).

A quality model is presented in standard (ISO, 1999), according to which software is evaluated with a set of internal, external and quality in use metrics. In this case software quality is defined as the total set of properties that determine software capability to satisfy assigned requirements in accordance with its purpose.

The application area of external quality metrics is validation and expert evaluation of the software. The group of external quality characteristics and metrics corresponding to them describe the programming product that is completed and ready for use. In order to evaluate software quality the standard (ISO, 1999) defines six groups of external and internal characteristics.

1. Functionality is a set of software properties that determines its ability to execute the established functions.
2. Reliability is the set of properties that enable the software to retain its serviceability and to convert raw data into the desired result under predetermined conditions in an established period of time.
3. Usability is the set of properties that characterizes the necessary conditions of software use by users.
4. Efficiency is the set of properties that characterizes conformity of the software resources used to quality of execution of its functions.
5. Maintainability is the set of properties that characterizes the level of efforts needed to execute the required software modifications.
6. Portability is the set of properties that characterizes the adaptability of software to work in different functional environments.

The set of metrics that pertain to each group of higher level characteristics is again divided into several sub-characteristics. For example, the software reliability, which is defined as the capability of software to maintain its level of performance under stated conditions for a stated period of time, includes the following sub-characteristics:

a. Maturity is the set of indicators that describe frequency of occurrence remaining in the software.
b. Fault tolerance is the ability of software to retain a certain functioning level during the onset of software malfunctions.
c. Recoverability is the property of software to restore its ability to work (assigned level of functioning), and also program data.
d. Reliability compliance is the degree of software conformity to normative requirements for reliability (standards), and also to customer requirements.

The basic nomenclature, calculation sequence and scale of possible values for metrics of software quality that pertain to each group of quality products with reference to the lifecycle process in which the metric is used, and composition of the necessary documentation for determining input parameters for calculation are defined in (ISO, 2000).

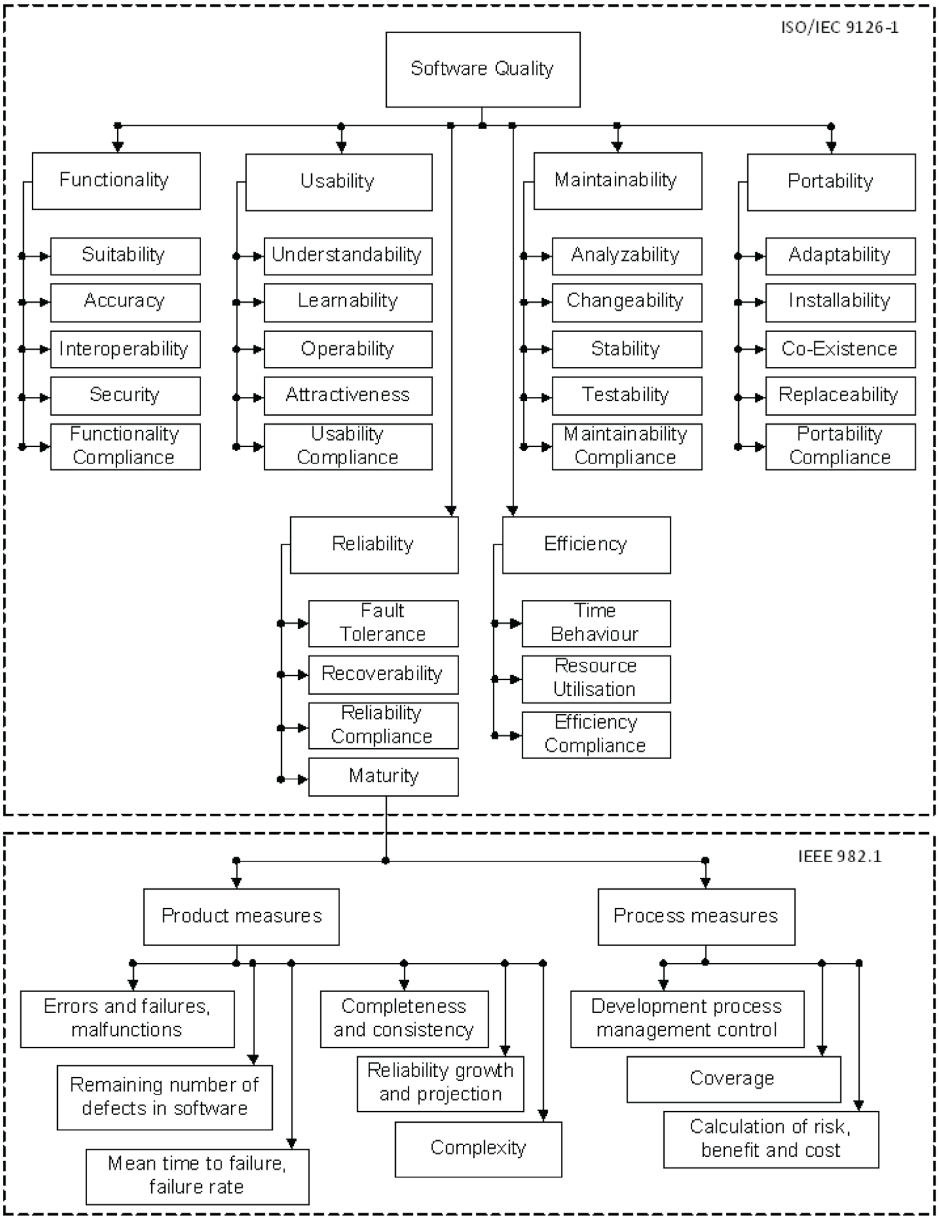
In addition to the listed categories the standard (IEEE, 1988, a) determines a number of functional groups that characterize different properties of reliability of the software itself (indicators, or product measures), as well as the design process (process metrics), based on which the reliability metrics are classified.

Examined standards can be used to create profiles of the evaluation and quality assurance of software. Figure 5 shows the interconnection of the standards IEEE 982.1-1988 (IEEE, 1988, a) and ISO/IEC 9126-1:1999 (ISO, 1999). The standard ISO/IEC 9126-1:1999 is fundamental and assures comprehensive inclusion of software quality. At the same time the standard IEEE 982.1-1988 allows one to assure more thorough analysis of software reliability as one of the top priority quality characteristics of software of information and control critical systems.

Based on an analysis of the classifications presented above for the systematic description of quality metrics and reliability a unified system of classification features is proposed (Figure 6). Development of the systemic classification of reliability metrics and software quality is a necessary condition of successful harmonization of normative documents and creation of effective methods of evaluation and assurance of quality of the software being developed.

Production and analysis of initial information for determining metrics: Analysis of the standards

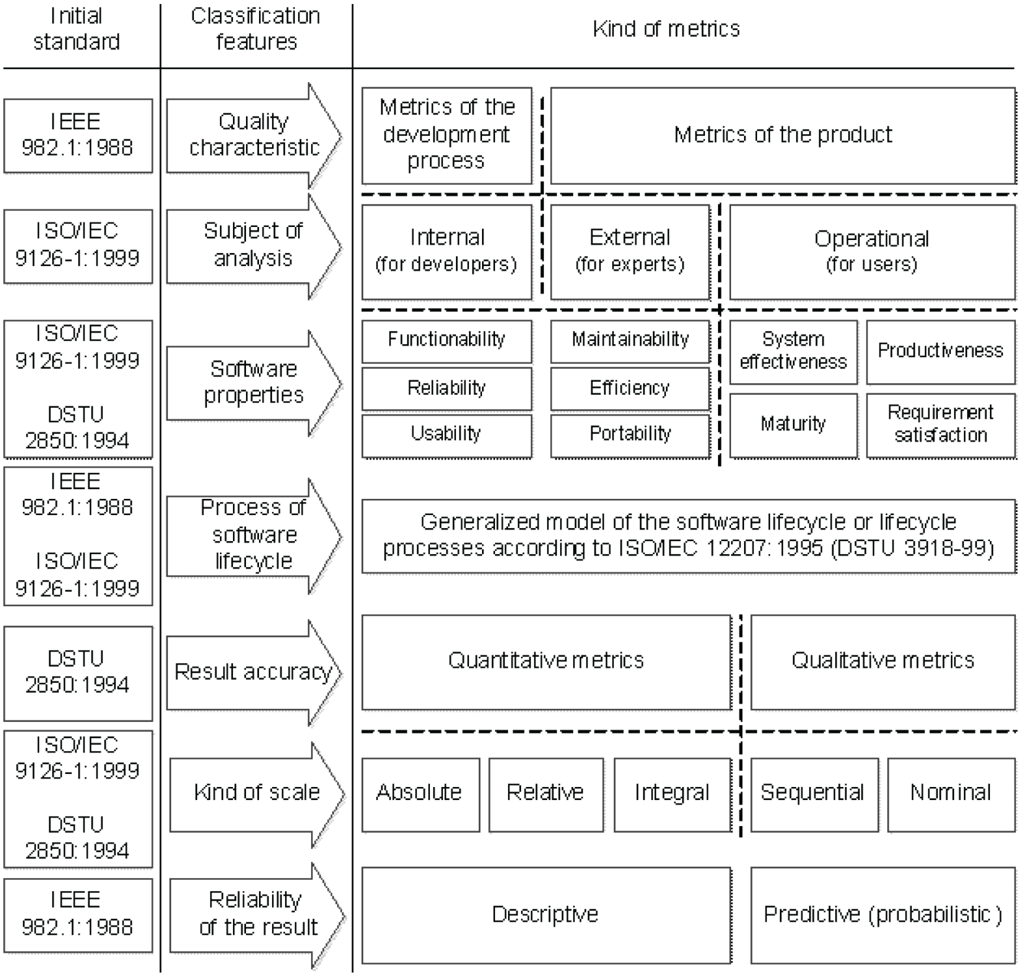
Figure 5. Interconnection and scopes of standards IEEE 982.1and ISO/IEC 9126-1



IEEE 981.1-1988 (IEEE, 1988, a) and IEEE 981.2-1988 (IEEE, 1988, b) allows to conclude that in order to determine input parameters for calculation of different metrics various information sources are required at the different stages of the software lifecycle. Among the main sources of information we can distinguish the following:

- General information on the software project. This includes dates of the beginning and completion of each step of the software lifecycle, description of processes of verification, number of releases (that is versions, outputs) of software and so forth. The reporting of general information on

Figure 6. Classification scheme of reliability metrics and software quality



the course of execution of the software design process is executed by the manager of the software project.

- The report on results of performing software verification after completion of each step of the software lifecycle. The report should include information on the nature of defects discovered, reason for their introduction and later discovery, time lost for preparation and conducting verification, and also information. The report is compiled directly by analysts-experts, as a rule manually.
- The report on software testing results. This includes information on time of discovery, level of seriousness and nature of software defects and information on reasons and time (date or stage of the software lifecycle) of the introduction of the corresponding defects, time of their correction, and also the test kits used, number of successful runs of the program and so forth. The report is compiled directly by test engineers manually or using automated recording devices.

- Technical description of the software release that is provided for testing or verification. This should include information on the overall number of procedures and functions (modules), number of modified, supplemented and deleted modules in comparison with the preceding release, and also the modular structure of the software for the possibility of converting the software to a state graph. The technical description is compiled directly by programming engineers, manually as a rule.
- The source code and executable code, which allow one to determine objective characteristics of the software; number of lines in the source code, size of the program, number of operators and operands used, and also the total number of their occurrence on the program and so forth. The software source code can be used along with corresponding utilities to produce a state graph of software as a whole and of individual modules. The software presentation in the form of a graph is necessary for calculating individual metrics and for developing test benches and executing the testing itself.
- Technical documentation for the software, which includes requirements for the software (specification), technical description and so forth. In calculating certain metrics the production of a comprehensive result requires that the experts propose evaluations or assignments of weighting factors (significance) for different software characteristics, input parameters or intermediate results. These factors can be determined based on analysis of corresponding sections of the software technical documentation.

Thus, the executed analysis allows one to insert additional classification features for quality metrics and their parameters: source of information for the determination of input parameters to calculate quality metrics (reports on fulfillment of verification and testing processes, technical description of the software release, source code and so forth); information compiler (project manager, system analysts, programmer-managers and test engineers and so forth); degree of objectivity (reliability and completeness) of the presented information.

It should be emphasized that the process of determining numerical values of input parameters for calculation of reliability metrics manually is unfeasible because of complexity and considerable amount of initial data. Therefore, the task of developing (or selection) support tools for gathering the initial information and automatic determination of input parameters for the calculation to metrics is needed. For this reason software source code analyzers are used as objective sources of information for determining input parameters for calculation of software quality metrics.

Based on the examined standards and analysis of publications (IEEE, 1988, a), (ISO, 2000) and (Pressman, 1997) a database of reliability indicators (metrics) and tools has been developed, which allows one to make a choice of indicators with consideration of the previously listed classification features, and also the stage of the lifecycle at which the reliability evaluation is made, and to produce their quantitative value. The calculation of measures is carried out by using deterministic methods of evaluation described in a standard (IEEE, 1988, b), while for calculation of predictive measures various probability reliability models can be used.

Evaluation of Software Development and Verification Processes

An evaluation of software development processes is accomplished by examination and analysis of documentation in accordance with the requirements for methods, devices and documentation of development described above (see Figure 4).

In this case, one can use special metrics, and the evaluation overall can be carried out and presented by means of radial metric diagrams.

The ratio of the number of software modules (or subsystems), which have been developed using such methods, to the total number of modules (subsystems) can be used as metrics for evaluating the fulfillment of requirements for the use of formal methods.

The quality of software development, fulfillment of requirements for the number of modules, complexity of relations among them can also be evaluated by using special metrics (for example, the Halstead metric, McCabe metric and others (Pressman,1997)).

It should be emphasized that evaluation of the fulfillment of requirements for software by nature is subordinate with respect to evaluation of verification, because these requirements are overall requirements for development and verification, or are checked directly together with evaluation of software verification. This pertains, in particular, to evaluation of the development results themselves, execution of requirements for methods and tools.

Tasks and criteria of software verification evaluation: The quality of conducting verification of software is of great significance for reliability and safety of the I&C system. The tasks of software verification evaluation are: analysis of software requirements based on requirements for the system and general requirements, which are determined by normative documents; check of the conformity of task formulations for software development to these requirements; quality check of the verification plan, test methods and their completeness in accordance with the tasks assigned to the software; the quality check of verification reports and their conformity to plans and methods.

One should note that these tasks, and also the tasks of evaluating the quality of their solution from the standpoint of fulfillment of requirements for safety, are not easy to formalize. Usually the verification analysis is accomplished by traditional methods of documentation analysis, and individual results can be checked by using specially developed tools. At the same time, considering the high criticality and importance of a maximally objective and complete evaluation of software verification, one must find approaches to the development of models that describe this process and allow one to improve its quality.

The process of software verification evaluation of I&C systems that are important for nuclear power plant safety can be constructed by means of (Kharchenko, 2000): formation and structuring of the full set of requirements for software, which must be checked in the verification process at different stages of the lifecycle; development of a system of criteria for evaluating software verification; compilation of a system of verification evaluation criteria and set of requirements established for the software; formalization of the verification analysis processes and its evaluation for basic criteria; creation and use of tools for support of software safety analysis during verification, licensing and expert analysis.

Criteria for verification is similar to the criteria of software evaluation represented above and includes the criteria of completeness, independence, successfulness, documentation and accessibility.

Software verification corresponds to the completeness criteria if during the verification the conformity of software to all requirements of specifications, standards and other normative documents was tested.

Software verification corresponds to the independence criteria in accordance with the software safety class. Thus, for class 2 verification is conducted by a group of specialists (organization), which are administratively and/or financially independent of the specialists (organization), which developed the software.

Software verification corresponds to the criterion of successfulness, if the verification was finished completely prior to placing the system in use, that is by this time all defects found were analyzed and eliminated (or a well-founded decision for their subsequent elimination was made).

Software verification corresponds to the criterion of documentation if a plan and report were issued which describe in detail the course and results of verification. In this case individual parts of a verification plan and report, which have individual significance (programs, test methods, protocols and so forth) can be issued in the form of individual documents.

Software verification corresponds to the accessibility criterion if all of the documentation on software verification was set forth in a form understandable to specialists who do not participate in conducting the development and verification.

Evaluation of documents related to software development: During the expert evaluation of documents on software development the requirement specification and design documentation are evaluated. In the expert analysis of the requirement specification the following are established and evaluated: the extent to which software requirements are correct and not contradictory; to what extent the functional requirements for software correspond to requirements for the I&C system; how fully are general requirements for software reflected in the feasibility study (requirements, which are established independently of specific functional purpose of the I&C system).

The evaluation of software requirements is conducted with consideration of: safety class of the I&C system, which includes software is a component; level of software approval; software purpose.

During expert examination of the design documentation one will analyze: description of the composition, structure and functions of component parts of the software; information on methods and means of testing and running experiments with software.

The evaluation of verification documents: The basic verification documents for evaluation are verification plan and verification report.

The software verification plan (SVP) evaluation is conducted based on criteria of documentability, accessibility, completeness, independence.

1. In the evaluation based on documentability criterion one establishes that the SVP was issued prior to the beginning of software verification and defines: choice of verification strategy; sequence of conducting verification; methods and devices used in the verification process; sequence of documentation of verification actions; sequence of verification results evaluation.
2. In the evaluation based on accessibility criterion one establishes that the SVP is set forth in a form understandable for specialists who did not participate in the software development process.
3. Based on the completeness criterion one carries out the evaluation of the following items stipulated in the SVP:
    a. Sequence of conducting verification. In evaluating the sequence of conducting verification one must establish that the verification stipulates after each step of the software development: generation of requirements for software; design; coding.
    b. Completeness of tests. In evaluating the completeness of tests it should be established that the sets of tests that are selected for verification will assure the possibility of checking all stipulated functions and interfaces of the I&C system, and also the check of fulfillment of requirements for software.
    c. Software verification and development tools. In evaluating the tools of software verification and development it should be established that the SVP stipulates the use of automated design and testing tools and indicates the selection criteria for them. One should evaluate the conformity of the proposed criteria

to the requirements of norms, rules, standards and recommendations; in particular, when using automated tools to generate code one must check that the given tools have gone through verification with the same requirements as the software itself.

d. Particular features of the verification of different kinds of software.

4. For an evaluation based on the independence criterion it should be established that in the SVP: for software of I&C system of safety class 2 it is stipulated that verification will be carried out by a group of specialists (organization), who are administratively and/ or financially independent of the specialists (organization) that developed the software; for software of I&C system of safety class 3 it is stipulated that the verification will be conducted by specialists who have not participated directly in development of the software (administrative and financial independence is not required), or by software developers on the condition that the review and evaluation of the verification results will be done by independent specialists.

Comments and recommendations made during the expert examination must be considered in the final version of the SVP, which is used in performing the software verification.

Evaluation of the software verification report (SVR) is conducted based on criteria of documentability, accessibility, completeness, independence and successfulness.

1. In the evaluation based on the criterion of accountability one should establish the fulfillment of requirements for the SVR structure, which should contain: lists of input and output signals during software tests; results of tests and their evaluations; deficiencies discovered during tests; conclusions based on results of analysis of the discovered deficiencies and measures to eliminate them, and also to evaluate the degree of detail of the documentation of all stages of the software verification process.
2. In the evaluation based on the criterion of accessibility one should establish that the SVR is set forth in a form that can be understandable for specialists who did not participate in the software verification process.
3. According to the completeness criterion one will evaluate the conformity sequence, strategy and order of conducting verification, methods, tests and software verification tools used that are stipulated in the SVP and actually used (reflected in the SVR).
4. In the evaluation based on the independence criterion one should compare the independence of the specialist (organization) that conducted the verification as stipulated in the SVP and the actual dependence from the specialist (organization) that developed the software.
5. Based on the successfulness criterion one will check correctness of the evaluation of results of each test and establish that all deficiencies discovered in the course of the software verification are recorded, analyzed, eliminated and results of subsequent evaluations are presented.

Tools to Support Evaluation

There are the following classification features for tools: functional purpose of the tool; degree of process automation; number and nomenclature of lifecycle stages and processes, supported by the tool; project components (its components or stages of development, verification or expert examination), supported by the tool; degree of intelligence; possibility of integrating a given tool with other tools.

These features allow classifying of tools as follow.

1. By functional purpose one can distinguish tools for informational, analytical, and organizational support.
2. By degree of process automation tools can be subdivided into manual (partially formalized), automated, and automatic. In determining the type of tool based on this feature one must consider the degree of automation of preparation, input, analysis, documentation and display of information.
3. By the number of supported stages tools are divided into local, compositional, and end-to-end. This feature determines the boundaries and scope of the operation of a tool.
4. By kind of project components one can distinguish tools that support evaluation of: products (requirements, specifications, design components, codes, methods, reports and so forth); processes (specification, design, coding, testing, verification and so forth).
5. By level of intelligence one can distinguish: non-intelligent tools, or traditional kind of tools (without using knowledge-based methods); intelligent tools; and combined tools.
6. According to possibility of integration tools are divided into integratable, which allow one to use a given tool together with other ones, and non-integratable.

By grouping the different (by purpose, level of intelligence and so forth) tools it is possible for carrying out various scenarios of the expert examination, which require use of analytical, information and organizational type tools, intelligent or combined tools and so forth.

Informational tools are intended for the generation, preliminary processing and analysis of information required for carrying out independent verification and expert examination of software and, as a rule, are automated, local or composite tools of non-intelligent or combined type, which support, above all, verification and expert examination of products.

Tools of this kind provide:

1. Generation of a profile-like base of national and international normative documents, which determine the software requirements and order of evaluating their execution during verification and software expert examination.
2. The generation of general and particular normative profiles of software based on an analysis of profile-like documents:
    a. Software requirements (structure and properties; inspection and diagnostics; reliability and tolerance; development; verification).
    b. Methods of evaluating the fulfillment of requirements.
    c. Evaluation of the quality of the process and expert examination results.
3. The formalized analysis of the general and functional requirements for the software that has been examined by experts based on the submitted documents.
4. Formalized preparation of data on the expert analyzed software and processes of its development and verification based on templates (questionnaires).
5. Databases on software expert examination that have been carried out and are being carried out, which include full systematized information on tasks, expert analysis object, course and results of the expert examination.
6. A transition from verbal to formal description of software requirements (partially formalized verbal matrices, semantic trees, product rules, Z-notations).
7. Databases of quality metrics and software reliability.
8. Database of software reliability models.

Results of execution of the informational tools are databases of profile-like documents, metrics, models, expert examinations; normative profiles; standardized plans of the verification and its evaluation; completed templates (questionnaires).

The questionnaires and templates are used to run individual procedures of the expert examination and verification in accordance with chosen methods.

Analytical tools are intended for carrying out direct analysis of software and to evaluate conformity of the verified (expert analyzed) software to established requirements, reliability of verification and expert examination and are automatic local tools that are both intelligent (combined) and non-intelligent, which support primarily verification and expert examination of products.

Analytical tools support:

1. Verification of normative profiles (completeness, correctness and consistency of the general requirements) of the software designs being developed and analyzed by experts.
2. Statistical analysis of software.
3. Dynamic testing of software.
4. Selection and rating of metrics and reliability measures (quality) of software.
5. Selection and verification of software reliability models.
6. Analysis of the fulfillment of general and functional requirements for expert analyzed software.
7. Analysis of the reliability and safety of software based on standardized methods.
8. Evaluation of the completeness, reliability and other characteristics of independent verification and expert examination.

Results of running the analytical tools are technical reports on verification of normative profiles; static and dynamic testing of software; selection and rating of metrics, measures and models of software reliability; analysis of the fulfillment of requirements for expert analyzed software; evaluation of characteristics of reliability, completeness and resources for carrying out independent verification and expert examination.

Organizational support tools are intended for planning, organizing and controlling the process of independent verification and expert examination and are automated or manual, local or composite tools of the non-intelligent type, which support verification and expert examination of processes and products.

Tools of this kind use as initial information normative documents; design documentation; data and results of running information and analytical tools.

Organizational support tools provide:

1. Planning of the expert examination (tasks, schedules, resources, personnel).
2. Timely analysis of the course and results of the expert examination.
3. Management of expert analysis process.
4. Documenting the results of the expert examination (partial and summary reports).
5. Analysis and evaluation of the quality of the process for conducting independent verification and expert examination of software.

Results of running the organizational support tools are general planning documents; diagrams of work execution while conducting independent verification and expert examination of software; technical reports on the course, results of independent verification and expert analysis, evaluation of the process of carrying them out; summary reports.

It should be emphasized that at the present time tools of the analytical type have been the most popular for evaluation of software, which support the solution of statistical analysis and software dynamic testing tasks.

Solutions and Recommendations

Specific features of software development and usage require proper regulation requirements towards the program components.

At the same time requirement to software should be agreed with requirements to I&C system. Categories of functions performed by I&C system have influence with software requirements, including requirements for composition of the functions, quality, reliability, stability, interaction with other components, procedures and processes.

Therefore developing of requirements for software components shall be done taking into account features of target I&C system, international and national regulatory requirement. For the solution of this issue systematic approach and methods, supported with appropriate tools, are required.

Modern model-based methods and techniques should be applied to assess NPP I&C software, in particular, model-checking (Lahtinen et al., 2010) and invariant-oriented evaluation (Kharchenko (Ed), 2012), software safety analysis techniques (Hui-Wen Huang et al., 2011) etc.

FUTURE RESEARCH DIRECTIONS

To match the latest trends and industry requests software components of I&C systems become more complex. Development of software engineering technologies also opens up new aspects and generates new issues for designing and implementation of software. Therefore possible implications of new programming technologies must be analyzed to ensure timely and adequate adaptation and clarification of regulatory frameworks.

Also attention should be paid to the fact that in large projects of I&C systems several organizations with different background and possibly from different countries can participate. Thus harmonization of requirements and ensure their adequate interpretation may be beyond the common regulatory aspect. In this scope, issues of personnel training, establishment of effective communications between the development teams and the utilities and other become important.

All these issues require systematic study and comprehensive scientific researches.

CONCLUSION

1. Software is a specific object for safety regulation. It is a component of I&C system to which requirements are applicable, and also it is a means of ensuring the satisfaction of regulatory requirements. At the same time software is the most likely sources of common cause failures. Therefore the need to minimize risks of common cause failures is reflected in the requirements to processes of software development and verification, as well as application of diversity.
2. Standardization, evaluation and assurance of software safety should be based on process-and-product-approach. I.e. harmonized requirements for the program as a product and the processes related to the creation, evaluation and use of programs at various stages of the lifecycle should be used.
3. Degree of completeness, adequacy and correctness of requirements to software is the determining factor in assessing their compliance, and thus ensure the quality, reliability and safety of both software and I&C system of NPP.
4. Methods that are used for software evaluation should be standardized and cover all aspects of software development and application. If it is necessary, correct application of such methods can be evaluated by experts. From this point of view special significance is acquired by criterion of documentation.

REFERENCES

Adziev, A. V. (1998). Myths about software safety: Lessons of famous disasters. Open systems, 1998, vol. 6. Retrieved December 16, 2012, from http://www.osp.ru/os/1998/06/179592/

Aizenberg, A., & Yastrebenetsky, M. (2002). Comparison of safety management principles for control systems of carrier rockets and nuclear power plants. *Space Science and Technology*, *1*, 55–60.

Anderson, R. B. (1979). *Proving Programs Correct*. New York: Wiley.

Ben-Ari, M. (2000). *Understanding programming languages*. Wiley.

DSTU-2850 (1994) Computer software – Metrics and methods for quality assessment. Ukrainian state standard.

Everett, W., Keene, S., & Nikora, A. (1998). Applying Software Reliability Engineering in the 1990s. IEEE Transactions on Reliability 50th Anniversary Special Publication, 47 (3-SP), 372-378.

Huang, H.-W., Wang, L.-H., Liao, B.-C., Chung, H.-H., & Jiin-Ming, L. (2011). Software safety analysis application of safety-related I&C systems in installation phase. *Progress in Nuclear Energy*, *6*(53), 736–741. doi:10.1016/j.pnucene.2011.04.002

IEC 60812 (2006). Analysis technique for system reliability – Procedure for Failure Mode and Effects Analysis (FMEA). International Electrotechnical Commission.

IEC 60880 (2006). Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. International Electrotechnical Commission.

IEC 61025 (2006). Fault tree analysis. International Electrotechnical Commission.

IEC 61508 (2008). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. International Electrotechnical Commission.

IEEE 610.12 (1990). Standard Glossary of Software Engineering Terminology. Institute of Electrical and Electronics Engineers.

IEEE 982.1 (1988). Standard Dictionary of Measures to Produce Reliable Software. Institute of Electrical and Electronics Engineers.

IEEE 982.2 (1988). Standard Guide of Measures to Produce Reliable Software. Institute of Electrical and Electronics Engineers.

ISO. IEC 9126-1 (1999). Information technology. Software product quality – Part 1: Quality model. International Organization for Standardization.

ISO/IEC TR 9126 (2000). Information technology. Software product quality – Part 2: External metrics; Part 3: Internal metrics; Part 4: Quality in use metrics. International Organization for Standardization.

Kersken, M. (2001). Qualification of pre-developed software for safety-critical I&C application in NPP's. Paper presented at CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, Hluboka-nad-Vltavou, Czech Republic.

Kharchenko, V. S. (Ed.). (2012). CASE-assessment of critical software systems. Quality. Reliability. Safety. Kharkiv, Ukraine: National Aerospace University KhAI.

Kharchenko, V. S., & Vilkomir, S. A. (2000). The Formalized Models of Software Verification Assessment. Paper presented at 5th International Conference Probabilistic Safety Assessment and Management, Osaka, Japan.

Lahtinen, J., Valkonen, J., Bjorkman, K., Frits, J., & Niemela, I. (2010). Model checking methodology for supporting safety critical software development and verification. Paper presented at ESREL 2010 Annual Conference, Rhodes, Greece.

Lawrence, S., Hatton, L., & Howell, C. (2002). *Solid Software*. Prentice Hall.

Lyu, M. R. (1996). *Handbook of software reliability engineering*. McGraw-Hill Company.

NS-G-1. 1 (2000). Software for computer based systems important to safety in nuclear power plants. Vienna, Austria: IAEA.

Pressman, R. S. (1997). *Software Engineering: A Practioner's Approach*. McGraw-Hill Company.

Vilkomir, S., & Kharchenko, V. (2000). An "asymmetric" approach to the assessment of safety-critical software during certification and licensing. Paper presented at ESCOM-SCOPE 2000 Conference, Munich, Germany.

Vilkomir, S. A., & Kharchenko, V. S. (1999). Methodology of the review of software for safety important systems. In G. I. Schueller, P. Kafka (Eds). Safety and Reliability. Proceedings of ESREL'99 - The Tenth European Conference on Safety and Reliability (pp. 593-596). Munich-Garching, Germany.

ADDITIONAL READING

IAEA. (1999, b). Verification and validation of software related to nuclear power plant instrumentation and control. Technical reports series Nº384. IAEA, Vienna.

IAEA - TECDOC-1328. (2002). *Solutions for cost effective assessment of software based instrumentation and control systems in nuclear power plants*. Vienna: IAEA.

IEC 62340 (2008). Instrumentation and Control Systems Important to Safety – Requirements to Cope with Common Cause Failure.

NUREG (2008) Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems. NUREG/CR-7007. *Office of Nuclear Regulatory Research, NRC, 2008.*

Pullum, L. (2001). *Software fault tolerance techniques and implementation*. ARTECH HOUSE.

Sterpone, L. (2008). Electronics System Design Techniques for Safety Critical Applications. *Lecture notes in electrical engineering. Springer Science + Business Media B.V., 2008.*

KEY TERMS AND DEFINITIONS

Common-Cause Failure (CCF): Failure of two or more structures, systems or components due to a single specific event or cause.

Common-Mode Failure (CMF): Failure of two or more structures, systems and components in the same manner or mode due to a single event or cause.

Diversity: Presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.

Fault Tolerance: Is the ability of software to retain a certain functioning level during the onset of software malfunctions.

Fault Tree Analysis (FTA): Deductive technique that starts by hypothesizing and defining failure events and systematically deduces the events or combinations of events that caused the failure events to occur.

Failure Mode, Effects and Criticality Analysis (FMECA): Is a reliability evaluation/design technique which examines the potential failure modes within a system and its equipment, in order to determine the effects on equipment and system performance.

Off-the-Shelf (OTS) Software Component: Pre-developed software components, usually developed by other organization and designed for specific solutions.

Chapter 6
Diversity and Multi-Version Systems

Alexander Siora
Research and Production Corporation Radiy, Ukraine

Vladimir Sklyar
Research and Production Corporation Radiy, Ukraine

Vyacheslav Kharchenko
National Aerospace University named after N.E. Zhukovsky KhAI,
& Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Eugene Brezhnev
Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

ABSTRACT

To protect safety-critical systems from common-cause failures that can lead to potentially dangerous outcomes, special methods are applied, including multi-version technologies operating at different levels of diversity. A model representing different diversity types during the development of safety-critical systems is suggested. The model addresses diversity types that are the most expedient in providing required safety. The diversity of complex electronic components (FPGA, etc.), printed circuit boards, manufacturers, specification languages, design, and program languages, etc. are considered. The challenges addressed are related to factors of scale and dependencies among diversity types, since not all combinations of used diversity are feasible. Taking these dependencies into consideration, the model simplifies the choice of diversity options. This chapter presents a cost effective approach to selection of the most diverse NPP Reactor Trip System (RTS) under uncertainty. The selection of a pair of primary and secondary RTS is named a diversity strategy. All possible strategies are evaluated on an ordinal scale with linguistic values provided by experts. These values express the expert's degree of confidence that evaluated variants of secondary RTS are different from primary. All diversity strategies are evaluated on a set of linguistic diversity criteria, which are included into a corresponding diversity attribute. The generic fuzzy diversity score is an aggregation of the linguistic values provided by the experts to obtain a collective assessment of the secondary RTS's similarity (difference) with a primary one. This rational diversity strategy is found during the exploitation stage, taking into consideration the fuzzy diversity score and cost.

DOI: 10.4018/978-1-4666-5133-3.ch006

INTRODUCTION

To guarantee required level of dependability, safety and security of computer-based systems for critical (safety-critical, mission-critical and business-critical) applications a diversity approach is used. This approach implies development, choice and implementation of a few diverse design options of redundant channels for created system. Probability of CCF of safety-critical systems may be essentially decreased due to selection and deployment of different diversity types on the assumption of maximal independence of redundant channels realizing software-hardware versions.

Risk of CCF is the main factor of reducing redundant I&C systems dependability. Diversity and defense-in-depth is the required principle of development for NPP I&C systems important for safety, first of all, reactor trip systems (Jonson, 2010).

Diversity is the general approach used for decreasing CCF risks of I&C systems, because differences in hardware and software components, development and verification technologies, implemented functions, etc. can mitigate the potential for common faults (Jonson, 2010, NUREG/CR-6303, 1994).

One of the key theoretical and practical problems is diversity estimation and optimization of used version redundancy capacity. Diversity related decisions should be made at the first design stages, because ones affect safety and cost of NPP I&C system. There are risks of the inaccurate or untrustworthy assessment of diversity and I&C system safety as a whole.

If diversity indicator is overstated, it causes increasing risks of CCF. If result of assessment is understated, it increases costs unreasonably at the production, implementation and operation stages.

This circumstance calls for that a lot of international and national standards and guides contain the requirements to use diversity in safety-critical systems, first of all, in NPP I&Cs (RTS), aerospace on-board equipment (automatic/robot pilot, flight control systems), railway automatics (signalling and blocking systems), service oriented architecture (SOA)-based web-systems (e-science) etc. (Pullum, 2001; Wood et al., 2009; Gorbenko et al., 2009; Kharchenko et al., 2010; Sommerville, 2011).

BACKGROUND

In a modern world, there are many various regulations, which, in general case, cover the most important areas widely used by the mankind. It is possible to distinguish those related (in some way) to safety important I&C systems, grouped into several sets to cover general issues of critical I&C systems at various lifecycle stages (including their development, operation and maintenance), security, as well as covering various technology-related aspects.

Application of the modern information and electronic technologies and component-based approaches to development in critical areas, on the one hand, improve reliability, availability, maintainability and safety characteristics of digital I&Cs. On the other hand, these technologies cause additional risks or so-called safety deficits. Microprocessor (software)-based systems are typical example in that sense. Advantages of this technology are well-known, however a program realization may increase CCF probability of complex software-based I&Cs. Software faults and design faults as a whole are the most probable reason of CCFs. These faults are replicated in redundant channels and cause a fatal failure of computer-based systems. It allows to conclude that "fault-tolerant" system with identical channels may be "non-tolerant" or "not enough tolerant" to design faults. For example, software design faults caused more than 80% failures of computer-based rocket-space systems, which were fatal in 1990 years (Kharchenko et al., 2003) and caused 13% emergencies of space systems and 22% emergencies of carrier rockets (Tarasyuk et al., 2011).

The CCF risks may be essential for diversity-oriented or so-called multi-version systems (MVSs) (Kharchenko, 1999) as well if choice of a version redundancy type and development of channel versions are fulfilled without thorough analysis of their independence and assessment of real diversity degree assessed by special metrics, for example, β-factor (Bukowsky & Goble, 1994).

COMMON EVENT AND COMMON CAUSE FAILURES

CCF is an event, when e_f (two or more) channels (versions) of redundant e-channel (e-version) system fail simultaneously, and there is a common reason caused this event. Thus, CCF is a multiple failure (MF). It is an alternative of a single failure (SF). On the other hand, multiple failures occur as a result of not only one (common) cause. Multiple failures may be caused by an influence of a few different reasons if these reasons concur or spread of influence time value is less than a speed of on-line testing and reconfiguration means. In this case MF may be called a common time failure (CTF). Hence, CCF and CTF are multiple failures or common event failures (CEF).

Attributes of the classification form simple hierarchy. CCFs and CTFs may be additionally divided in two groups in accordance with a number of failures (partial and full CCFs, i.e. PCCFs and FCCFs, and partial and full CTFs, i.e. PCTFs and FCTFs) and distinguishability of channel output data on failures, i.e. distinguishable (DCCFs, DCTFs) and undistinguishable (UDCCFs, UDCTFs) failures.

Authors of works related to NPP safety problems, first of all, attend to CCFs analysis. However, CTFs are the important objective of a research, as there are examples of serial failures caused by attacks on vulnerabilities of redundant channels and other reasons. Besides, a very important problem, in our opinion, is the analysis of distinguishability of effect failures, because it allows determining the moment of partial or full CCFs (or CTFs) by simple means of channel output data comparison.

ANALYSIS OF DIVERSITY RELATED STANDARDS

There are the following standards and guides contained requirements to diversity:

- **IEC 61513:** 2001. NPPs - I&Cs important to safety – general requirements for systems.
- **IEC 60880:** 2006. NPPs - I&Cs important to safety - SW aspects for computer-based systems performing category A functions.
- **IAEA NS-G-1.3:** 2002. I&Cs important to safety in NPPs.
- **IEEE std.7-4.3.2:** 1993. IEEE standard criteria for digital computers in safety systems of NPPs.
- **NUREG/CR-6303:** 1993. Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.
- DI&C-ISG-02, Diversity and Defense-in-Depth Issues, Interim Staff Guidance, BTP 7-19, Guidance for Evaluation of D&DiD In Digital I&C Systems (USA).
- **NP 306.5.02/3.035:** 2000. Requirement on nuclear and radiation safety to I&Cs important to safety in NPPs (Ukraine), etc.

These standards contain general requirements concerning: systems which must/should be developed using the diversity approach (RTSs); types of diversity used to develop NPP I&Cs and to decrease CCF probability; features of the diversity implementation, determination of types and volume of the diversity; assessment (justification) of real level of the diversity in developed systems;

drawbacks and benefits connected with the use of the diversity.

The standards are not enough detailed to make all necessary decisions concerning the diversity. It's important to develop additional detailed techniques of assessing diversity and choosing optimal kinds and volume of the diversity according to criterion "safety-reliability-cost."

NEW CHALLENGES OF DIVERSITY IMPLEMENTATION IN NPP I & C SYSTEM

Technology and Risks

Modern software/microprocessor (MP)-based and hardware/mixed FPGA-based technologies ensure new possibilities for implementation of the diversity approach (DA), because their application allows to use two additional kinds of the diversity:

- FPGA vs MP (main system is developed using FPGAs, diverse system is developed using MPs).
- FPGA1 vs FPGA2 (different manufacturers Altera, Xilinx, Actel (Microsemi), etc., subtechnologies SRAM, Flash, Antifuse, development techniques are used to develop main and diverse systems) (Kharchenko et al., 2011; Kharchenko et al., 2008).

The technologies of FPGA projects development, in particular graphical scheme and library blocks in CAD environment, special hardware describing languages (VHDL, Verilog, Java HDL, etc), microprocessor emulators, which are implemented as IP-cores allow increasing a number of possible options of different project versions and multi-version I&Cs. But they can create additional risks and deficits of safety or transform pre-existed ones caused by features of FPGA technology. Hence, they stipulate necessity to analyze and decrease such risks, to use positive features of new technologies.

Uniqueness of Multi-Version Systems

There are a lot of DA implementations in critical domains (Kharchenko et al., 2011) but:

- MVS component failures occur rarely; it does not allow to use statistical methods to evaluate reliability indicators.
- Comparative analysis of failures for different applications is not enough.

It concerns both MP-based and FPGA-based MVSs, but MP-based NPP I&C systems are operated more than forty years, when FPGA-based are operated during last ten-twelve years and are more unique.

Key questions are:

- How we should collect, compare experience of different domains and take into consideration features of DA applications?
- Is long time of non-failure operation reliable proof?

Standards Related to D3 Principle

A lot of standards and technical reports contain requirements to diversity and recommendations regarding to assessment of MVSs: IEC and IAEA standards (IEC 61513: 2001, IEC 60880: 2006, IAEA NS-G-1.3: 2002, etc), IEEE standards and NUREG guides (IEEE std.7-4.3.2:1993, NUREG/CR-6303:1994, NUREG/CR-7007:2009, etc.), EPRI reports (EPRI 1019183:2009, EPRI 1019181:2009, EPRI 1019182:2009), some national guides, for example (NP 306.5.02/3.035: 2000).

The requirements of these documents concern:

- NPP I&C systems which must/should be developed and produced using diversity approach.
- Diversity types to decrease a common cause failure probability of NPP I&Cs.
- Features, benefits and limitations of DA implementation.
- Postulation of necessity regarding: determination of the required diversity volume; assessment (justification) of the real diversity level; risks associated with the use of the diversity.

Existed standards are not enough detailed to make the assessment procedure. The most representative document is NUREG 7007. The main questions are the following:

- What should be specification and severity of regulation for DA implementation?
- How regulated should be requirements and procedures of assessment and development of FPGA-based NPP I&Cs?

Safety Assessment

There is a problem of CCF risks assessment and MVS safety assessment as a whole. Inaccurate assessment either increases risk of a fatal failure (understated assessment) or increases risk of unreasonable costs.

The main question is the following: what indicators (metrics), techniques and tools we should use:

- To assess the actual diversity level and MVS safety.
- To assess cost and limitations of developing and implementing such structures.
- To compare different structures of MVS according to a criterion “safety-cost” and make optimal decision?

CCF Risk Decreasing and MVS Safety

There is a problem of decreasing number of common version faults (CVF). The CVF number (and probability of CCF) may be decreased using several types of the diversity (multi-diversity or “diversity of diversity”).

There are problems of a compatibility and dependence of diversity types. Main questions are the following:

- What type (types) of diversity should be used?
- How much versions developers should use to ensure required level of the MVS safety?
- How to take into account dependencies of diversity types and to search regularized set of decisions (sets of diversity types)?

Challenges: Some Conclusions

There are two main theoretical and practical problems of the diversity approach application in NPP I&C systems. Firstly, a problem of the actual diversity level assessment for developed MVSs, reliability safety and taking into account:

- Product/process technologies (types, rate of physical, design and interaction faults).
- System architectures (type and capacity of the applied diversity and redundancy).

Second problem is a choice of product-process diversity types, MVS architecting and configuration of diverse components, etc.

WORK RELATED ANALYSIS

Known works, related to the current problem and taking into account features of NPP I&C systems, are divided into three groups: (1) classification and analysis of version redundancy types and diversity-oriented decisions; (2) methods and techniques of the diversity level assessment and evaluation of multi-version systems safety in context of CCFs; (3) multi-version technologies of safety critical systems development.

1. A set of diversity classification schemes (general, software and FPGA-based) was analyzed in (Kharchenko et al., 2009). First one is based on NUREG technical reports and guides, samples two-level hierarchy and includes seven main groups of version redundancy (Wood et al., 2009): a signal diversity (different sensed reactor or process parameters, different physical effects, different set of sensors); a equipment manufacture diversity (different manufacturers, different versions of design, different CEC versions, etc); a functional diversity (different underlying mechanisms, logics, actuation means, etc); a logic processing equipment or architecture diversity (different processing architectures, different component integration architectures, different communication architectures, etc); a logic or software diversity (different algorithms, operating system, computer languages, etc); a design diversity (different technologies, approaches, etc); a human or life cycle diversity (different design organizations/companies, management teams, designers, programmers, testers and other personnel). Software diversity types are classified in according to following attributes (Pullum, 2001; Volkoviy et al., 2008): life cycle models and processes of development (for example, V-model for main version and waterfall model with a minimum set of processes for duplicate version); resources and means (different human resources, languages and notations, tools); project decisions (different architectures and platforms, protocols, data formats, etc). Next one FPGA-based classification includes the following types of the diversity (Kharchenko & Sklyar, 2008; Siora et al., 2009): the diversity of electronic elements (different electronic elements manufactures, technologies of production, electronic elements families, etc); the diversity of CASE-tools (different developers, kinds and configurations of CASE-tools); the diversity of projects development languages (different graphical scheme languages, hardware description languages and IP-cores); the diversity of specifications (specification languages) and others.
2. There are following methods of the diversity level assessment and evaluation of the MVS dependability and safety (Kharchenko et al., 2009). Theoretical-set and metric-oriented methods are based on: an Eiler's diagram for sets of version design, physical and interaction faults (including vulnerabilities for assessment intrusion-tolerance); a matrix of diversity metrics for sets of different faults (individual, group and absolute faults of versions); calculation of diversity metrics by use of Eiler's diagrams or other data about results of testing and faults of different versions. Probabilistic methods use reliability block-diagrams (RBDs), their modifications (survivability and safety block-diagrams), Markovian chains, Bayesian method, etc. Statistical methods include the following procedures: receiving and normalization of version fault trends using testing data; choice of software reliability growth model (SRGM) taking into account features of version development and verification processes and fitting SRGM parameters; metrics diversity assessment; calculation of reliability and safety indicators. Fault injection-based assessment consists of: receiving project-oriented fault profiles; performing of faults injection procedure; proceeding of data and metrics diversity calculation; calculation of reliability and safety indicators. Expert-oriented methods use two groups of metrics: diversity

metrics for direct assessment of versions and MVS reliability and safety (direct diversity metrics); indirect diversity metrics (product complexity metrics and process metrics); values of these metrics may be used to assess direct diversity metrics. Expert methods are added to other techniques founded on interval mathematics-based assessment of diversity metrics and MVS indicators, soft computing-based assessment (fussy logic, genetic algorithms), risk-oriented approach and so on.

3. Multi-version technologies (MVTs) of diversity types selection and application, development of MVSs as a whole are based on (Siora et al., 2009; Wood et al., 2009) use of diversity types and strategies table, a model of multi-version life cycle (MVLC), a special graph of diversity types and their modifications, and procedures of diversity type and volume choice according to different criteria. The set of developed diversity strategies (Wood et al., 2009) consists of three families of strategies: different technologies—Strategy A (digital vs analog), different approaches within the same technology—Strategy B (MP vs FPGA) and different architectures within the same technology—Strategy C (IP-based vs VHDL). Each of the strategy families is characterized by combinations of diversity criteria that may provide adequate mitigation of potential CCF vulnerabilities according to metrics determined in an expert way.

There are a lot of examples of multi-version systems and multi-version technologies application in different safety critical areas. Generalized results of MVS application analysis are presented by the matrix "types of diversity – areas of multi-version I&Cs application" in Table 1 (Wood et al., 2009; Kharchenko et al., 2010).

Types of diversity (diversity redundancy) are classified according to NUREG 6303 and painted by different colors. Last row of the matrix corresponds to other types of diversity. MVSs are used in space systems (Shuttle, ISS), aviation equipment (MC JVC, FAA FCS, Airbus and Boeing on-board systems), railway automatics (signaling, centralization and blocking systems SCB), chemical industry (CCPS), defense systems, power plants (electricity grid), NPPs (RTS and ESFAS), e-commerce and e-science (web-systems with diverse target web-services).

Table 1. Matrix "types of diversity – areas of multi-version I&Cs application"

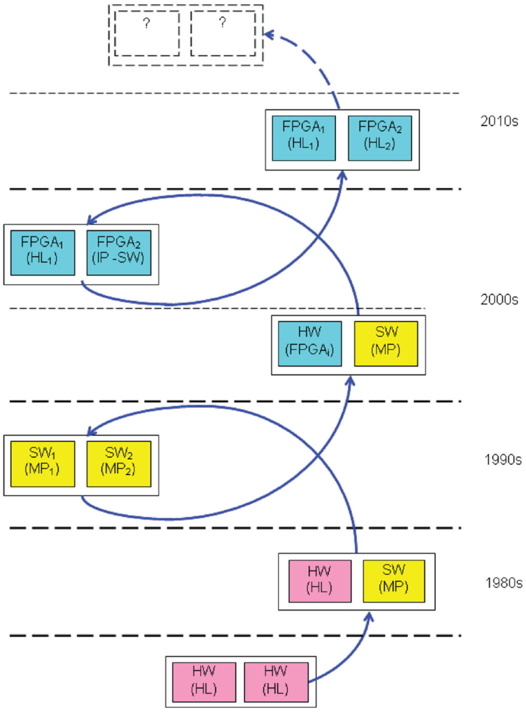
Diversity types	**Multi-version I&C systems application**												
	Space		Aviation				Rail. ways	Chemic. industry	Defense	Power Plants	NPPs		e-Commerce
	Shuttle	ISS	MC JVC	FAA FCS	Air-bus A320	Boeng 777	SCB	CCPS	MICS	Electr. Grid	RTS	ESFAS	WSOA
Design				■	■			■			■	■	■
Equipment		■		■	■	■	■	■			■	■	■
Function	■	■		■	■	■	■	■	■		■	■	■
Human	■	■	■	■	■	■	■	■	■	■	■	■	■
Signal							■	■			■	■	
Software	■		■	■	■	■		■			■	■	■
Others	■	■	■	■	■	■					■		

A LAW "NEGATION OF NEGATION": STAGES OF DIVERSITY APPROACH IMPLEMENTATION EVOLUTION IN NPP I&CS

Interesting are the results of transformation of multi-version I&Cs for the last decades in context of hardware-software-FPGA technologies development. There are a few diversity implementation evolution stages in safety-critical NPP I&Cs, in particular, reactor trip systems. Analysis of these stages allows formulating (or demonstrating truth) a law "negation of negation" (Kharchenko et al., 2009) (Figure 1):

- **Stage 1 (1970-1980s):** Use of hardware (hard logic, HL)-based one-version systems and transition from hardware (HW)-based systems with identical subsystems to systems with hardware (HL)-based primary subsystem and software (MP)-based secondary subsystem; it was the first "negation;"

Figure 1. Stages of diversity approach implementation evolution in safety-critical NPP I&Cs



- **Stage 2 (1990s):** Use of primary and secondary subsystems with software (SW) diversity (I&C platforms produced by Siemens, WH and other companies); example of multi-version systems with software diversity is two-version system consisting of subsystems developed using microprocessors Intel and Motorola (languages C and Ada); it completed the first cycle of "negation of negation;"
- **Stage 3 (2000s, first half):** Transition to FPGA-based primary and software-based secondary subsystems with equipment, design and software diversity (first generation of the I&C platforms produced by RPC Radiy); it was next "negation;"
- **Stage 4 (2000s, second half):** Application of FPGA-oriented soft processors for a primary subsystem and FPGA project developed using HDL-oriented language (hard logic) for creation of a secondary subsystem (next generation of the I&C platform produced by RPC Radiy); it completed the second cycle of "negation of negation;"
- **Stage 5 (beginning of 2010s):** Application of different FPGAs (hard logic) produced by different manufacturers (and other types of diversity) for primary and secondary subsystems correspondingly; it is next "negation."

What will be the next step? Probably, advancement of electronic technologies, in particular, nanotechnologies, naturally dependable, safe and secure chips will create new perspectives and possibilities for development of diversity-oriented decisions. Actel, Altera and other companies inform about creating first chips called nano FPGAs allowing to develop fault-tolerant projects using large-scale means.

AN EVOLUTION OF FPGA TECHNOLOGY AND DIVERSITY APPLICATION IN NPP I&CS

Complex Electronic Components and FPGA Technology for NPP I&Cs Development

An analysis of development and introduction trends of computer technologies to NPP I&Cs has specified a number of important aspects affecting their safety, peculiarities of development, update and licensing. Such trends include, among others (Yastrebenetsky, 2004): introduction of novel complex electronic components (CECs); expanded nomenclature of a software applied and increased effect of its quality to I&Cs safety; realization of novel principles and technologies in I&Cs development; advent of a large number of novel standards regulating the processes of I&Cs development and safety assessment. During recent decades the application of microprocessor techniques in NPP I&Cs design has substantially expanded. Microprocessors are used both in a system computer core and in realization of intellectual peripherals – various sensors, drives and other devices with built-in programmable controllers.

Another contemporary trend is dynamically growing application of programmable logic technologies, particularly, FPGA in NPP I&Cs, onboard aerospace systems and other critical areas. FPGA as a kind of CECs is a convenient mean not only in realization of auxiliary functions of transformation and logical processing of information, but also in execution of basic monitoring and control functions inherent in NPP I&Cs. This approach in some cases is more reasonable than application of software-controlled microprocessors (Kharchenko&Sklyar, 2008). In assessment of FPGA-based I&Cs it should be taken into consideration that application of this technologies somewhat levels the difference between hardware and software, whereas obtained solutions are an example of a peculiar realization of so called heterosystems – systems with a "fuzzy" software-hardware architecture and mixed execution of functions. This circumstance and other features of FPGA technology increase a number of diversity types and enlarge a set of possible diversity-oriented decisions for NPP I&Cs.

FPGA Peculiarities in Context of Dependability and Safety

FPGA architecture topologically originates from channeled Gates Arrays (GA). In FPGA internal area a set of configurable logic units is disposed in a regular order with routing channels there between and I/O units at the periphery. Transistor couples, logic gates NAND, NOR (Simple Logic Cell), multiplexer-based logic modules, logic modules based on programmable Look-Up Tables (LUT) are used as configurable logic blocks. All those have segmented architecture of internal connections.

System-On-Chip architecture appeared due to two factors: a high level of integration permitting to arrange a very complicated circuit on a single crystal, and an introduction of specialized hardcores into FPGA. Additional hardcores may be: additional Random Access Memory (RAM) units; JTAG interface for testing and configurating; Phase-Locked Loop (PLL) – a frequency control system to correct timing relations of clock pulses as well as for generation of additional frequencies; processor cores enabling creation of devices with a control processor and a peripheral.

An analysis of dependability assurance possibilities in FPGA-based systems permit to determine the following FPGA peculiarities (Kharchenko & Sklyar, 2008; Bobrek et al., 2009).

1. Simplification of development and verification processes: an apparatus parallelism in control algorithms execution and realization of different functions by different FPGA elements; an absence of cyclical structures in FPGA projects; an identity of FPGA project

presentation to initial data; advanced testbeds and tools; verified libraries and Intellectual Properties (IP) - cores in FPGA development tools.

2. There are three technologies of FPGA-projects development: development of a graphical scheme by means of library blocks in CAD environment; development of a software model by means of especial hardware describing languages (VHDL, Verilog, Java HDL, etc); development of a program code for operation in the environment of microprocessor emulators, which are implemented in FPGA as IP-cores. It does allow increasing a number of options of different project versions and multi-version I&Cs.
3. Assurance of fault-tolerance, data validation and maintainability due to use of: redundancy for intra- and inter-crystal levels; diversity implementation; reconfiguration and recovery in the case of component failures; improved means of diagnostic.
4. Security assurance: FPGA reprogramming is possible only with use of especial equipment. Stability and survivability assurance due to: tolerance to external impacts (electromagnetic, climatic, radiation); possibilities of implementation of multi-step degradation with different types of adaptation.

FPGA Technology Application in Safety-Critical Systems and NPP I&Cs

Due to these peculiarities area of FPGA technology application has essentially expanded. We can say about an affirmative answer to question "Expansion of FPGA-technology application in safety-critical systems for the last decades: evolution or revolution?" It is confirmed by (Bakhmach et al., 2009):

- A substantial increase of applying the technologies based on programmable logic (FPGA, CPLD, ASIC).
- The FPGA technology is improved and ensures new possibilities to develop more reliable and effective systems; application of the FPGA technology for development of military (B-1B, F-16, etc) and civil aircraft control systems (Boeing 737, 777, AN70, 140), space control systems (satellites FedSat, WIRE; the Mars-vehicle Spirit), etc.
- The application of FPGAs in NPP I&Cs (Ukraine, Russia, Bulgaria: 1999-start, 2002 – 1000, 2006 – 6000, 2008-2010 – more than 8000 chips every year).

Besides, the illustration of FPGA expansion is an evolution of the NPP I&Cs produced by RPC Radiy during 2000-2008 years (Kharchenko & Sklyar, 2008).

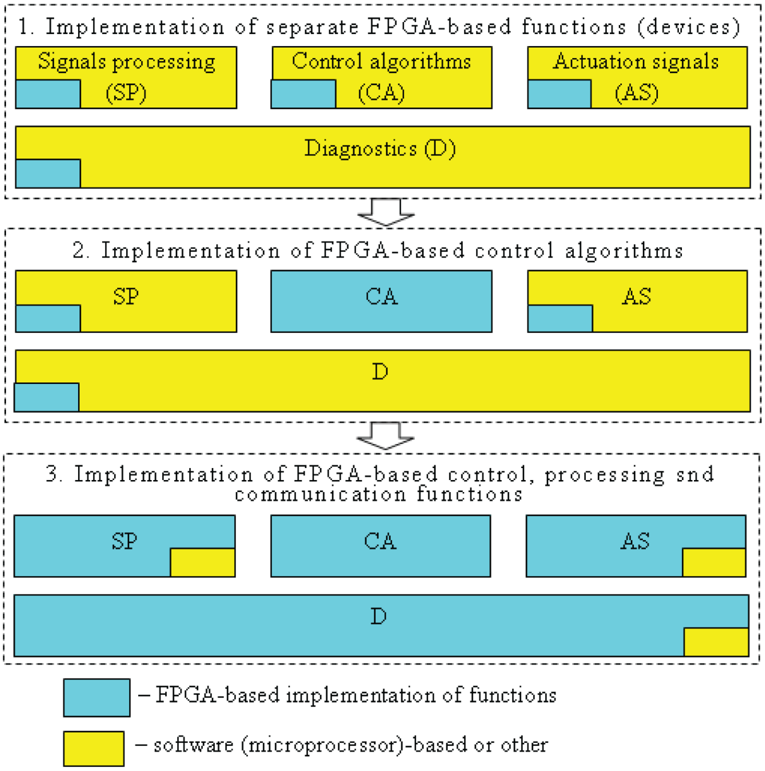
There are three stages of the evolution (Figure 2): from implementation of separate FPGA-based functions in I&Cs (signals processing (SP), control algorithms (CA), actuation signals formation (AS) and diagnostics (D), stage 1, and implementation of FPGA-based CA, stage 2, to preferred implementation of FPGA-based SP-, CA-, AS-, D- and communication functions, stage 3.

An analysis of industrial application experience of FPGAs in NPP I&Cs is described in a technical report prepared by EPRI (Naser, 2009).

Key Challenges Connected with Diversity Application in FPGA-Based I&Cs NPP

Main conclusions concerning FPGA-based MVS development and implementation experience are the following: FPGA-based multi-version I&Cs are used in NPPs during 6-8 last years, i.e. these systems are a new object of analysis and still more unique one; the FPGA technology gives additional possibilities to develop MVSs and ensure

Figure 2. Application of FPGA technology in the NPP I&Cs produced by RPC Radiy


1. Implementation of separate FPGA-based functions (devices)
Signals processing (SP)
Control algorithms (CA)
Actuation signals (AS)
Diagnostics (D)
2. Implementation of FPGA-based control algorithms
SP
CA
AS
D
3. Implementation of FPGA-based control, processing snd communication functions
SP
CA
AS
D
– FPGA-based implementation of functions
– software (microprocessor)-based or other

high safety and reliability; processes of FPGA project development are similar to processes of SW-based project development. FPGA project product is similar to HW-based project product (hard logic); there are no any international standards determined requirements to use diversity for the I&Cs development and application taking into account FPGA features.

Results of a comparative analysis of challenges caused by development and application of software- and FPGA-based multi-version systems are presented in Table 2.

Table 2. Key challenges for software-based and FPGA-based MVSs

Challenges	Software-Based Multi-Version I&C	FPGA-Based Multi-Version I&C
Detailed standards	There are standards determining general requirements to use of diversity	There are no special standards
Experience of development and operation	More 20 years	6-8 years
Trustworthiness of diversity assessment	Methods of expert-based, metrical assessment, probabilistic methods using SRGMs	Methods of expert-based, metrical, probabilistic (RBD), deterministic methods
Development of MVSs	Choice of diversity types, generation of really diverse software versions	Number of diversity types increases
Verification of MVSs	Verification activities volume are significantly increased	Verification is more simple due to simplifying of version verification

MAIN CONCEPTS AND MODELS OF MULTI-VERSION COMPUTING

Taxonomy Scheme of Multi-Version Computing

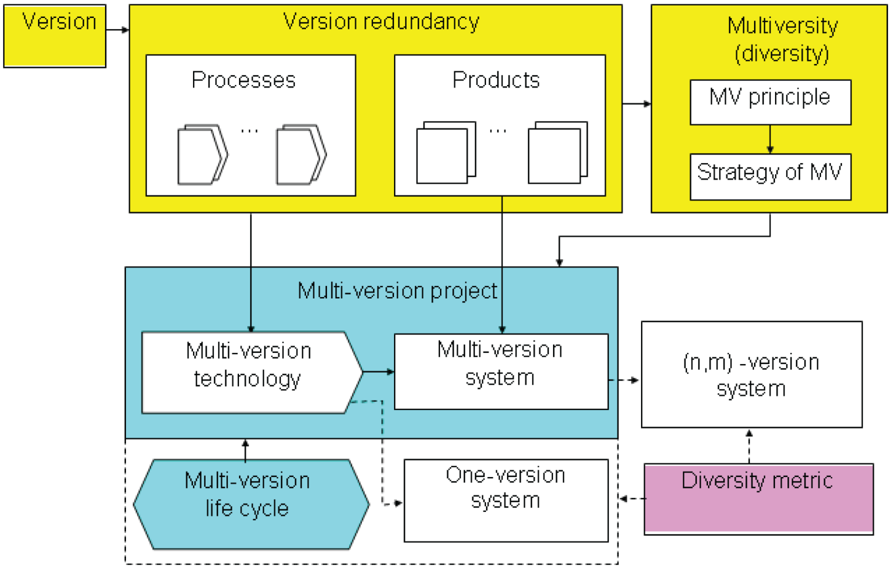
A set of concepts concerning the diversity may be united by a general term "multi-version computing" on the analogy with a "dependable computing" (Avižienis et al., 2004). Multi-version computing is a type of dependable computing organization based on use of the diversity approach. The taxonomy scheme of multi-version computing, developed taking into consideration concepts in this area, described in international standards, includes the following elements (Kharchenko et al., 2009) (Figure 3).

Version is an option of the different realization of an identical task (by use software, hardware or FPGA-based products and life cycle processes); an identical versions of structure redundancy-based system are trivial. Version redundancy (VR) is a type of product and process redundancy allowing to create different (non-trivial) versions; product VR is realized jointly with structure, time and other types of non-version redundancy.

Diversity or multiversity (MV) is a principle providing use of several non-trivial versions; this principle means performance of the same function (realization of products or processes) by two and more options and processing of data received in such ways for checking, choice or formations of final or intermediate results and decision-making on their further use.

Multi-version system (MVS) is a system, in which a few versions-products are used; one-version systems may be redundant but consist of a few trivial versions. Multi-diversion system (MDVS) is MVS, in which two or more VR types are applied. Multi-version technology (MVT) is set of the interconnected rules and design actions, in which in accordance with MV strategy a few versions-processes leading to development of two or more intermediate or end-products are used; thus, for development of MVS MVT should be used, for development of one-version systems multi-version and one-version technology can be used both.

Figure 3. Taxonomy scheme of multi-version computing



Multi-version project (MVP) is a project, in which the multi-version technology is applied (version redundancy of processes is used) leading to creation of one- or multi-version system (realization of version redundancy of products). Strategy of diversity (MV) is a collection of general criteria and rules defining principles of formation and selection of version redundancy types and a volume or/and choice of MVTs. Besides, important elements of the multi-version computing are concepts "multi-version life cycle," "diversity metric." More detailed interpretation of these concepts will be done below.

Diversity Type Classification Schemes

Different variants of diversity type classifications were described above. The analysis of the considered classifications allows approving that: they are presented by classifications of mixed facet-hierarchical or matrix (network) types; the NUREG-based classification presented in (Wood et al., 2009) is the most detailed and systematic, though the principle of attributes orthogonality is not sustained in full in it; for example, subsets of a design and software, a functional and signal version redundancy are crossed and dependent; a variety of a product (system, hardware and software components) and of a process (technologies of development, testing and maintenance) version redundancy cause complexity of VR selection and MVS development.

More general diversity type classification scheme is so-called "cube" of diversity described by a matrix MVR =|| vrijk|| in three-dimensional space (Figure 4). The scheme has coordinates: a stage of LC (i); a level of project decisions (PD, j) and a type of VR (project decision). Example of two-space matrix presented a cut of "cube" for FPGA-based systems is shown on the Table 3.

Figure 4. "Cube" of diversity-oriented decisions

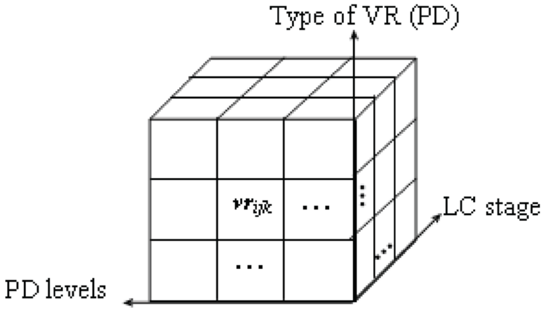


Table 3 contains variants of a joint application of one or two diversity types (items 1.4.2-1.4.4, 2.3.3-2.3.8, 3.3.3-3.3.8, 4.2.4-4.2.15; for example, last combinations correspond to 12 = 4 (kinds of EE diversity) x 3 (kinds of CASE-tool diversity)) couples.

Models Multi-Version Systems

One-version W(1) and multi-version W(n) systems are defined by 4 and 6 variables (Kharchenko et al., 2010):

$$W\left(1\right)=\left\{X,\ Y,\ Z.\ \Phi\right\}, \tag{1}$$

$$W\left(n\right)=\{X,\ Y,\ Z.\ \Phi,\ V,\ \Psi\}, \tag{2}$$

where X, Y, Z – sets of input signals, internal conditions (states) and output signals correspondingly; $\Phi = \{\varphi_i, i=1, ..., a\}$ – a set of I&C functions (for examples, actuation functions or algorithms of reactor trip system); $V = \{v_j, j=1, ..., n\}$ – a set of versions with output signals $Z_1, \ldots, Z_n$ (or signals Z_{id}, $d = 1, \ldots, n_i$; n_i is a number of versions for a function φ_i; $\forall\varphi_i \sim v_j = \{ v_{ij}, j=1,...,n_i\}$); $\Psi = \{\psi_s, s=1, ..., в\}$ – mapping $Z_i \to Z$.

If the function φ_i is performed, local mapping is true: $\psi_s{:}\{z_i(v_{i1}),..., z_i(v_{in_i})\} \to Z_i^{(S)}$ .Taking into account Equations 1 and 2, multi-version system and one-version system are connected by a relationship:

Table 3. Matrix of diversity-oriented FPGA-based decisions

Stages of FPGA-Based I&C Life Cycle	Kinds of Version Redundancy			
	1 Diversity of Electronic Elements (EE)	2 Diversity of CASE-Tools	3 Diversity of Project Development Languages	4 Diversity of Scheme Specification (SS)
1 Development of block-diagrams according to signal formation algorithms		1.2.1 Different develo-pers of CASE-tools 1.2.2 Different CASE-tools kinds 1.2.3 Different CASE-tools configurations		1.4.1 Different SSs 1.4.2-1.4.4 Combi-nation of couples of diverse CASE-tools and SSs
2 Development of program models of signal formation algorithms in CASE-tools environment		2.2.1 Different deve-lopers of CASE-tools 2.2.2 Different CASE-tools kinds 2.2.3 Different CASE- tools configurations	2.3.1 Joint use of graphical scheme language and HDL 2.3.2 Different HDLs 2.3.3-2.3.8 Combi-nation of diverse CASE-tools and HDLs	
3 Integration of program models of signal formation algorithms in CASE-tools environment		3.2.1 Different deve-lopers of CASE-tools 3.2.2 Different CASE-tools kinds 3.2.3 Different CASE-tools configurations	3.3.1 Joint use of graphical schemes and HDL 3.3.2 Different HDLs 3.3.3 – 3.3.8 Combination of couples of diverse CASE-tools and HDLs	
4 Implementation of integrated program model in FPGA	4.1 Different manufacturers of EEs 4.2 Different technologies of EEs production 4.3 Different families of EEs 4.4 Different EEs of family	4.2.1 Different deve-lopers of CASE-tools 4.2.2 Different CASE-tools kinds 4.2.3 Different CASE-tools configurations 4.2.4-4.2.15 Combina-tion of diverse CASE-tools and EEs		

$$W\left(n\right)=\{W\left(1\right),\ V,\Psi\}. \tag{3}$$

The system W(1) may be a structure-redundant and contain usual means Ψ for signals processing from identical channels (versions). In this case card V=1. For system W(n) is true that: $\forall_j=\overline{1,a}$: $\exists_j$: n_i>1.

The mapping ψ_s is generally described by: a subset of versions $\Delta v_s \subset v_j$ for receiving an output signal Z_i; a vector $\vec{t}_s$ of a version v_{ij} an initialization time ($\vec{t}_s$= {t(v_{i1}),..., (v_{in_i})}); a mean of transforming η_s values $z_i(v_{i1}),...,\ z_i(v_{in_i})$ in an output signal Z_i^S. Hence,

$\forall\psi_s \in \Psi : \psi_s$ = { Δvs, $\vec{t}_s$, η_s} and $Z_i^{(S)} = \eta_s\ [z_i(v_{ij}),\ \vec{t}_s\ ],\ v_{ij} \in \Delta v_s$.

There are the following means of transforming η_s: (a) the conjunctive, when $Z_i^S = \mathrm{V}z_i(v_{ij})$; (b) the time conjunctive, when $Z_i^S = \mathrm{V}z_i(v_{ij})\sigma_{ij}$, where σ_{ij}=1, if t=t(v_{ij}), and if not σ_{ij}=0; (c) the majority, when Z_i^S =M[$z_i(v_{ij})$], where M is a majority function k out of *l* (or k out of n); (d) the majority-weighted, when weights of versions $\omega(v_{ij})$ are additionally defined on majorization; (e) the functional, when $Z_i^S = f[z_i(v_{ij})]$, where f - some function of transforming output signals of every version.

The model (6.2) describes system with n versions that, $n = \sum_{i=1}^{a} n_i$. This model does not take into account the possibility of applying several diversity types. A set of version redundancy kinds $R=\{r_d, d=1,\ldots, m\}$ may be decomposed on subsets for versions of products $v_{prd}(t_j)$ and processes $v_{prc}(t_j)$: $R=(\bigcup_j \Delta R_{prdj}) \cup (\bigcup_j \Delta R_{prcj})$, where ΔR_{prdj} and ΔR_{prcj} – appropriate subsets.

Thus, different diversity types, r∈R, are accumulated in final versions of a multi-version system. It is described by a special mapping Θ: R → V. The mapping Θ may be presented by a Boolean matrix $\|\theta d_j\|$, $d = \overline{1,m}; j = \overline{1,n}$, where $\theta_{dj} = 1$, if diversity type r_p is used in version v_j, and if not $\theta_{dj} = 0$. Then a multi-version system W (n,m) or a multi-diversion system is described by the formula:

$$\begin{aligned} W(n,m) &= \{X, Y, Z, \Phi, V, \Psi, R, Q\} = \\ \{W(n), R, \Theta\} &= \{W(1), V, \Psi, R, \Theta\}. \end{aligned} \tag{4}$$

It is important to describe a correspondence between a set of versions V and a set of redundant channels $C=\{c_q, q=1,\ldots,l\}$. This correspondence may be defined by a mapping Q:V→ C. This mapping is presented by a Boolean matrix Q = $\|\omega_{jg}\|$, $d = \overline{1,m}$, $g = \overline{1,l}$, where $\omega_{gj} = 1$, if version v_i is realized by a channel c_j, and if not $\omega_{gj} = 0$. Then a model of multi-version (multi-diversion) system is the following:

$$\begin{aligned} W(n,m,l) &= \{X, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\} = \\ &\{W(n,m), C, Q\}. \end{aligned} \tag{5}$$

MVSs with temporal redundancy and p iterations of algorithms are indicated as W(n,m,n,p) a dividing number of parallel (structural) versions n_c, and sequential versions realized by using one channel. Set X may be decomposed for different versions if:

$$\begin{aligned} &x = \bigcup_j x_j, \forall j_1 j_2 \in \overline{1,n}, j_1 \neq j_2 : \\ &X_{j1} \cap X_{j2}, X_{j1} \cap X_{j2} = \phi. \end{aligned}$$

Such MVSs are called multi-version systems with a naturally divided input alphabet:

$$W_{NX} = \{ \{X_j\}, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\}. \tag{6}$$

If versions process data presented in different notations, such MVSs are called multi-version systems with an artificially divided input alphabet WAX. A special function-transformer Πx (Πxj) should be specified in addition to alphabet X:

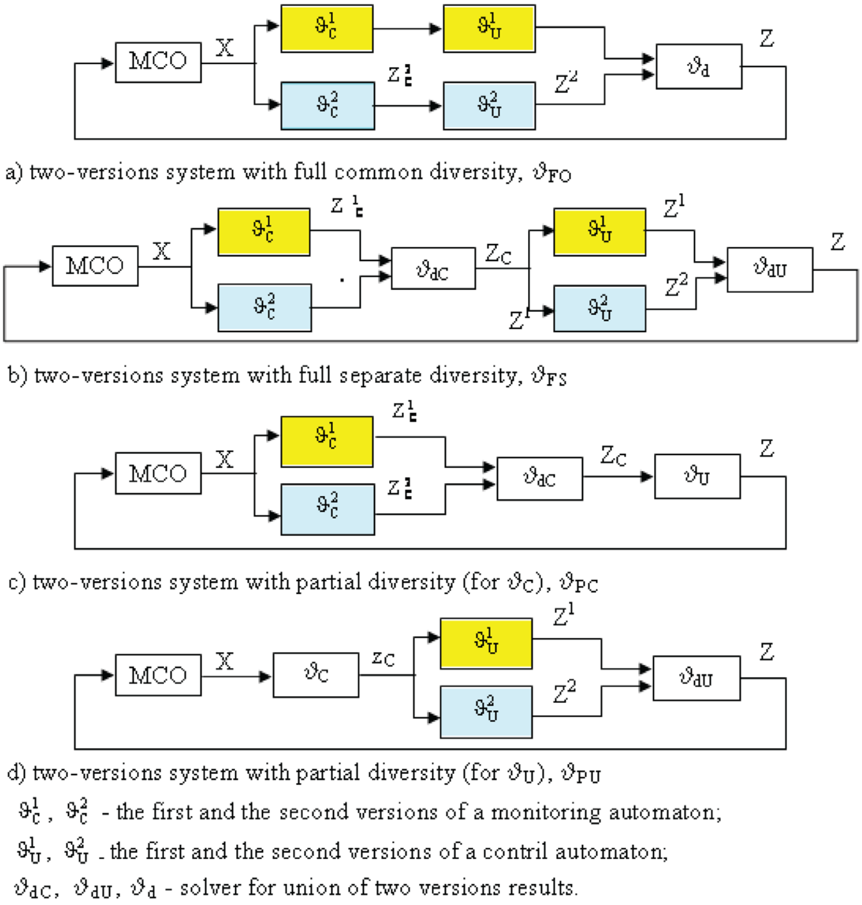
$$W_{NX} = \{X, \{\prod xj\}, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\}. \tag{7}$$

Besides, I&Cs performing safety-critical functions may be represented by a composition of two interconnected subsystems – a monitoring (checking) subsystem and a control subsystem (monitoring and control automata). Monitoring automaton ϑ_C analyses output signals X from a monitoring and control object (MCO) and forms its status code Z_C.

Control automaton ϑ_U forms control signals Z in accordance with signals Z_C. Several options of MVS architectures are possible for a FPGA-based I&Cs. Those options may be classified according to such attributes (see Figure 5):

- Degree of a diversity coverage (I&Cs with a full ϑF and partial ϑP diversity).

Figure 5. Architecture variants of two-version I&C systems



a) two-versions system with full common diversity, ϑ_{FO}

b) two-versions system with full separate diversity, ϑ_{FS}

c) two-versions system with partial diversity (for ϑ_C), ϑ_{PC}

d) two-versions system with partial diversity (for ϑ_U), ϑ_{PU}

ϑ_C^1, ϑ_C^2 - the first and the second versions of a monitoring automaton;

ϑ_U^1, ϑ_U^2 - the first and the second versions of a contril automaton;

ϑ_{dC}, ϑ_{dU}, ϑ_d - solver for union of two versions results.

- Diversity depth (I&Cs with a common ϑO and separate ϑS diversity); it should be noted that this feature is applicable only to the full system diversity.

Models of Multi-Version Life Cycle and Technology

A model of MVS life cycle (or multi-version LC model) is based on operations of the version generation G, the aggregation and selection U at various stages (Kharchenko et al., 2007). Example of the two-version life cycle model is shown on Figure 6 taking into account some FPGA-oriented design features (V_{ij} are different versions obtained on different stage of development) (Prokhorova et al., 2008).

In general case I&C system LC is a sequence of N stages. At each i-th stage of a multi-version I&C system LC Mi of diversity types may be applied. From Mi, i = 1,...,N; diversity types only a single j-th type, j = 1,...,Mi, may be selected. Besides, at each i-th stage of LC a single-version development technology may be selected. Each j-th diversity type at each i-th LC stage is characterized by two indices: diversity metrics (depth) dij and cost of a respective diversity type application (a cost increase as compared to a single-version option of each i-th LC stage).

Thus, a set of solutions on selection of diversity type is described by two matrices: diversity metrics values D = || d_{ij} || and cost values C = || c_{ij} ||. Hence, MVS LC may be presented as a bipolar N-level graph (Figure 7) called a graph of multi-version

Figure 6. FPGA-system multi-version life cycle

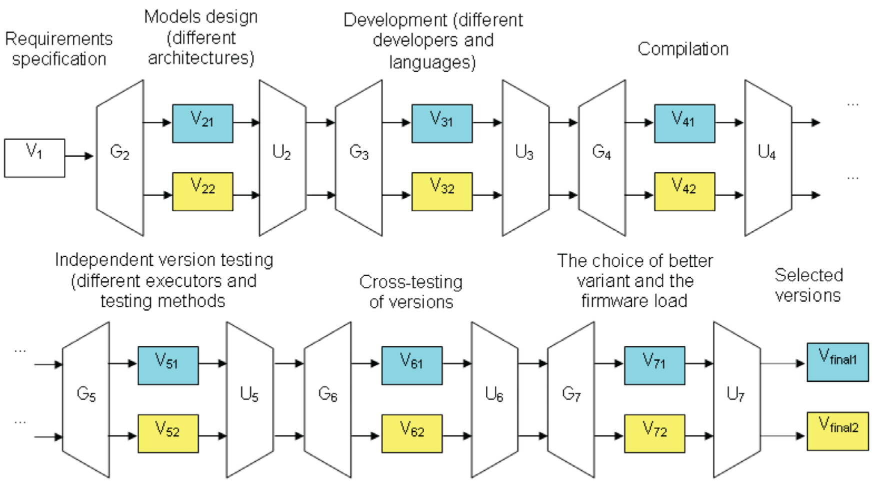
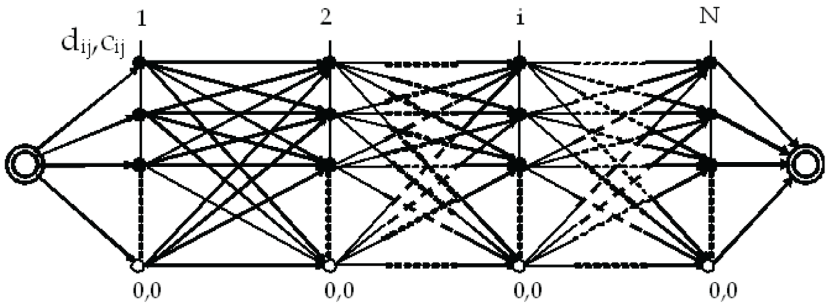

Requirements specification
Models design (different architectures)
Development (different developers and languages)
Compilation
V_1
G_2
V_{21}
V_{22}
U_2
G_3
V_{31}
V_{32}
U_3
G_4
V_{41}
V_{42}
U_4
...
...
Independent version testing (different executors and testing methods
Cross-testing of versions
The choice of better variant and the firmware load
Selected versions
...
...
G_5
V_{51}
V_{52}
U_5
G_6
V_{61}
V_{62}
U_6
G_7
V_{71}
V_{72}
U_7
V_{final1}
V_{final2}

Figure 7. Graph of MVTs



technologies (Sklyar & Kharchenko, 2007). MVT corresponds to a non-zero way in this graph.

Algorithms of MVT (optimal way in the graph) selection according to a criteria "diversity (safety)-reliability-cost" are described in (Kharchenko & Sklyar, 2008).

Development of Multi-Version Systems: Diversity with Dependencies

Complexity of the diversity type choice is caused by two reasons. First, the number of diverse version pairs is very large. It may be determined as a multiplication of cardinalities of sets for every attribute. Second, dependencies exist between different types of the diversity (e.g., between different manufacturers of chips and technologies of chips, between technologies and families of chips, etc.)

For example, application of Altera chips stipulates use of SRAM-FPGA technology-producing languages, VHDL, JHDL, Case-tool Quartus II, and their corresponding development and verification technologies. Application of Actel chips stipulates use of Flash-FPGA technology and Case-tool Libero. Conversely, VHDL and JHDL are also used in application of Actel chips and Libero tool. There are other dependencies between corresponding elements of FPGA- and microcontroller-based technologies in printed circuits board development technologies and manufacturers.

These dependencies, therefore, essentially complicate the task of the diversity type selection, and leads to the necessity of developing a model that allows for systematization of generation and choice of diversity type pairs.

Diversity model and algorithm: The model takes dependencies among diversity types into a consideration and simplifies the choice of diversity options.

A direct acyclic graph is used to represent the proposed model. Each node of this graph corresponds to some diversity type. Typically, several nodes are used for one diversity type to reflect dependencies. The edges are annotated (labeled) with sets of possible design decisions (values of diversity types). The order of nodes can be arbitrary. A path through the graph represents a set of feasible diversity decisions, which are independent within a given set. For each set, the possible diversity values are restricted according to labels of ongoing edges of the path through the graph, but these values have no dependencies inside the set and can be used in any combinations.

Based on diversity types presented in Table 4, an example of the diversity model is developed using abstract sets of diversity values. This makes the example more general and applicable for various types of computer systems. We consider seven diversity types (Table 4) and seven dependencies among the values of these types (Table 5), which are typical for many safety-critical systems.

Each dependency in Table 5 shows feasible combinations of diversity values. For example, dependency 1 means that if one of the values—TC1, TC2, or TC3—is chosen for diversity type TC, then only the values—MC1, MC2, or MC3—can be chosen for diversity type MC. Conversely, if diversity values TC4, TC5, or TC6 are being used, then only MC4 or MC5 can be used for MC.

For developing a diversity model, a subgraph splitting algorithm is used, which has previously been developed for software test generation (Vilkomir, 2009, Vilkomir, et al., 2009). In this section, the algorithm is adapted for a new task of a diversity model creation, and the meanings of nodes and edges are completely different, when compared with what was used for software test generation models. However, the algorithm used for model development here remains unchanged from earlier research.

The algorithm starts from a linear direct graph, which describes possible diversity values, but does not reflect any dependencies between these values. The graph is then modified by applying the algorithm in a cycle for each dependency. Each cycle includes four steps: splitting a subgraph, labeling ingoing and outgoing edges of split subgraphs, eliminating dead nodes and edges, and merging nodes. Developing a diversity model for diversity values from Table 4 with dependencies from Table 5 is considered below.

Developing a diversity model: Figure 8 represents different types of diversity (nodes) and sets of their possible values (ingoing edges). To design one subsystem (version) of a multi-version system, it is necessary to choose a specific value from each set. If there are no dependencies among diversity types, any combination of values is possible.

Because of dependencies, some combinations of diversity values are infeasible. To reflect de-

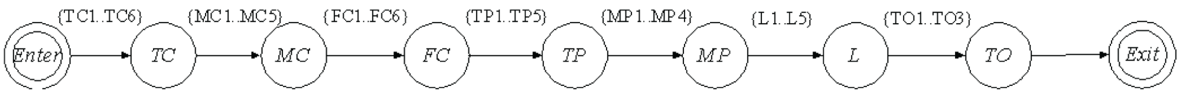
Table 4. Diversity types

Diversity Type	Diversity Values
TC	TC1, TC2, TC3, TC4, TC5, TC6
MC	MC1, MC2, MC3, MC4, MC5
FC	FC1, FC2, FC3, FC4, FC5, FC6
TP	TP1, TP2, TP3, TP4, TP5
MP	MP1, MP2, MP3, MP4
L	L1, L2, L3, L4, L5
TO	TO1, TO2, TO3

Table 5. Dependencies among diversity values

	Dependencies			
1	TC <----> MC	TC1, TC2, TC3	<---->	MC1, MC2, MC3
		TC4, TC5, TC6	<---->	MC4, MC5
2	MC <----> FC	MC1, MC2	<---->	FC1, FC2
		MC3, MC4, MC5	<---->	FC3, FC4, FC5, FC6
3	FC <----> TP	FC1, FC2, FC4	<---->	TP1, TP2
		FC3, FC5, FC6	<---->	TP3, TP4, TP5
4	TP <----> MP	TP1, TP3, TP5	<---->	MP1, MP2
		TP2, TP4	<---->	MP3, MP4
5	TC <----> L	TC1, TC3	<---->	L1, L2, L3
		TC2, TC4, TC5, TC6	<---->	L4, L5
6	L <----> TO	L1	<---->	TO1
		L2, L3, L5	<---->	TO2
		L4	<---->	TO3
7	TC <----> TO	TC1, TC3, TC5, TC6	<---->	TO1, TO2
		TC2, TC4	<---->	TO3

Figure 8. Model without dependencies



pendency 1 between TC and MC (Table 2), node TC is split and new labels for input and output edges are created (Figure 9), allowing only feasible combinations of TC and MC values. The formal rules for edge labeling can be found in (Vilkomir, et al., 2009).

To reflect dependency 2 from Table 5, node MC must be split. The result with new edge labels is shown in Figure 10. Note that that there is no connection between a lower TC and upper MC nodes. The reason is that this edge was labeled with the empty set at step 2 of the algorithm application. This means that a corresponding combination of diversity values is impossible. Such edges are considered as "dead" and are eliminated at step 3 of the algorithm application.

Figure 11 models dependency 3 between FC and TP nodes. Similar to the diagram in Figure

Figure 9. Model of dependency 1

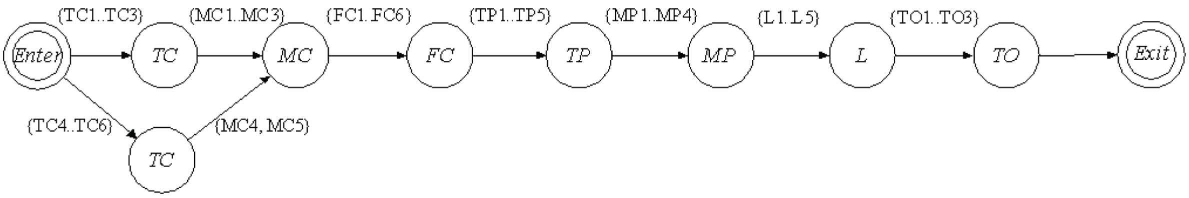


Figure 10. Model of dependencies 1 - 2

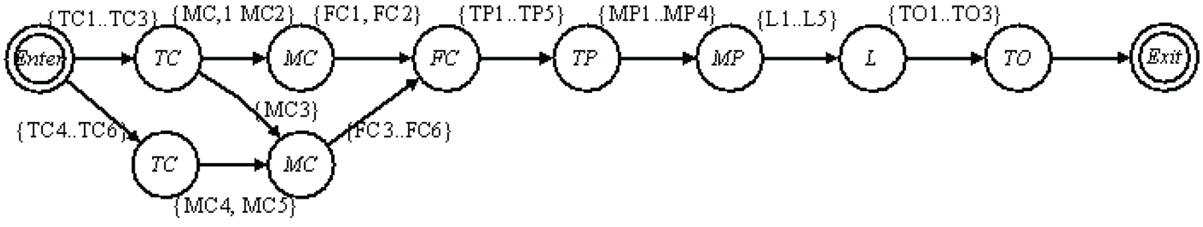
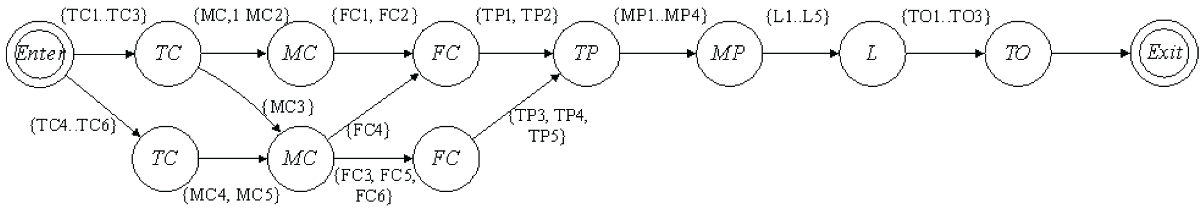


Figure 11. Model of dependencies 1 - 3



10 there is no connection between upper MC and lower FC nodes, because this edge is dead. Dependency 4 between TP and MP diversity types is reflected in Figure 12. Similar to all previous diagrams, the split subgraph contains only one node, in this case, TP.

To model dependency 5 according to the subgraph splitting algorithm, we need to split (duplicate) the subgraph, which contains all nodes between TC and L (9 nodes, including TC, but excluding L). Two edges and one node (marked with crosses in Figure 13) are dead and should be eliminated. The final diagram, which reflects dependency 5, is shown in Figure 14.

For dependency 6, between MP and L diversity types, node L should be split. This time, three instances of L (one old and two new) are used because three different "if - then" situations are involved in this dependency. Two dead edges are eliminated during the algorithm application. The model for this dependency is shown in Figure 15.

To model dependency 7, the subgraph with nodes between TC and TO is split. The process of dead nodes and edges elimination has now several cycles. The significant part of nodes and edges are eliminated as shown in Figure 16 (marked with black crosses for ingoing subgraph edges and red crosses for outgoing subgraph edges). The final model of the complete example is presented in Figure 17.

The example provided here contains seven diversity types and each type has from three to

Figure 12. Model of dependencies 1 - 4

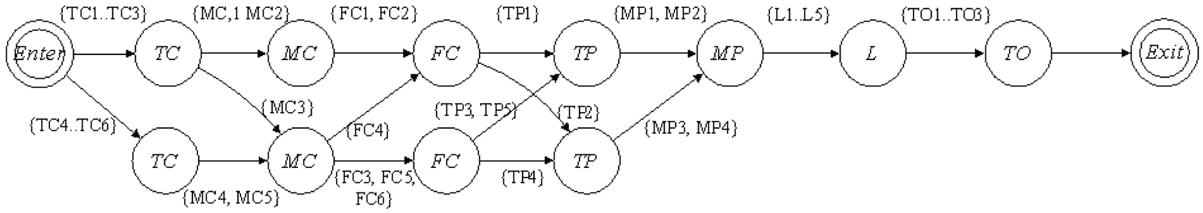


Figure 13. Eliminating dead nodes and edges for dependency 5

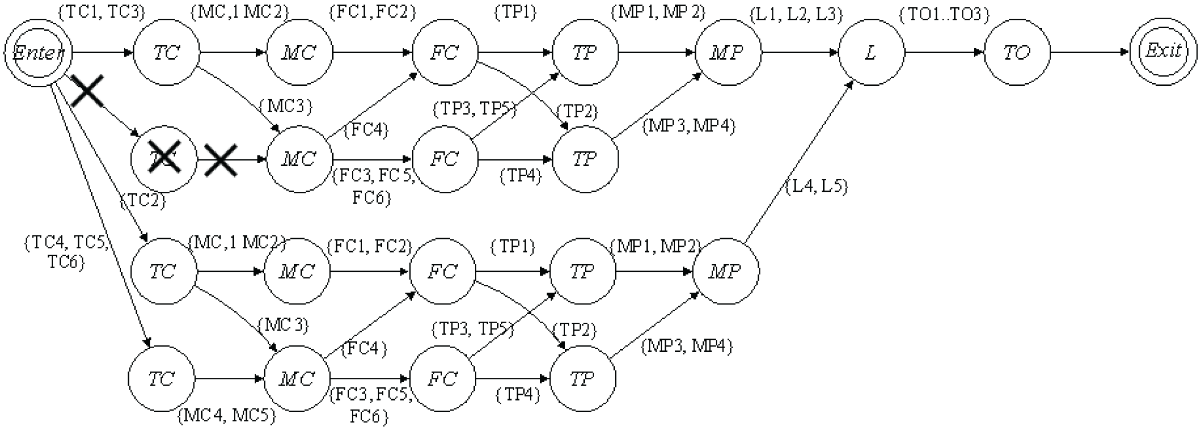


Figure 14. Model of dependencies 1 - 5

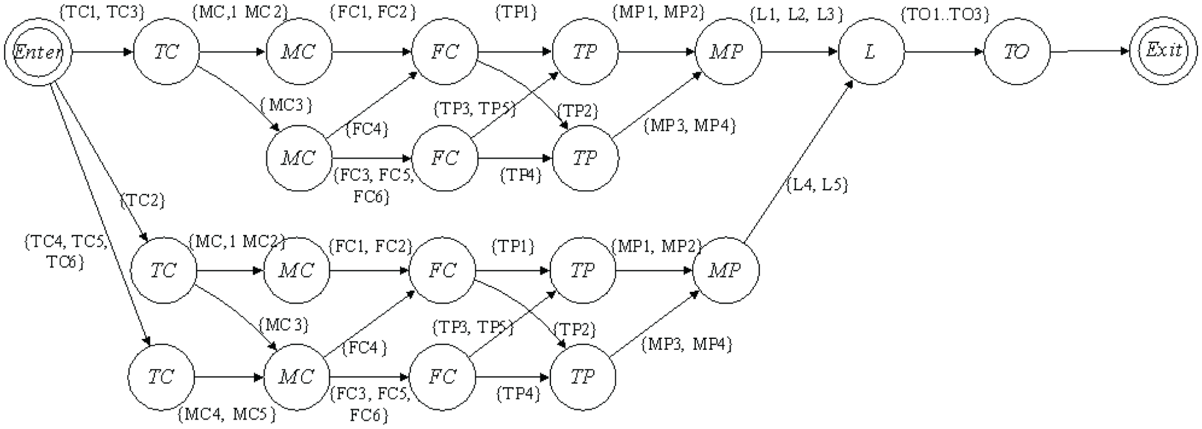


Figure 15. Model of dependencies 1 - 6

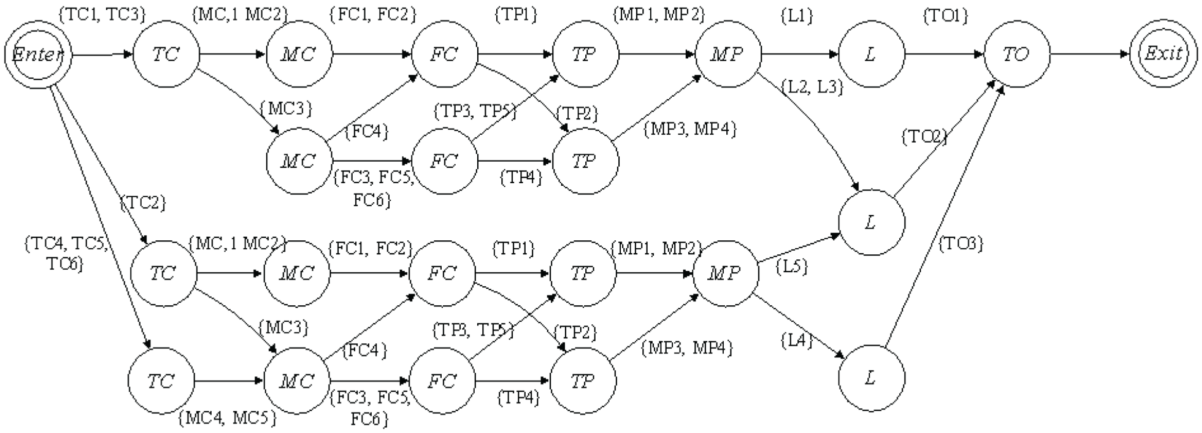


Figure 16. Eliminating dead nodes and edges for dependency 7

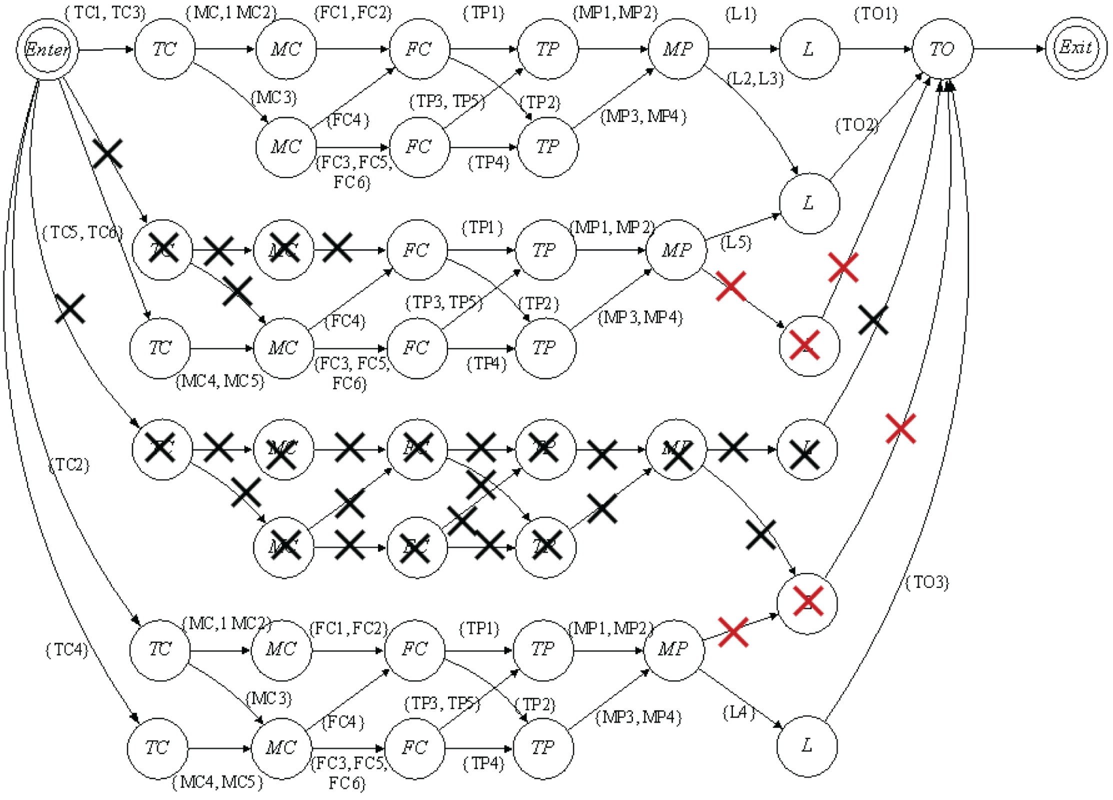
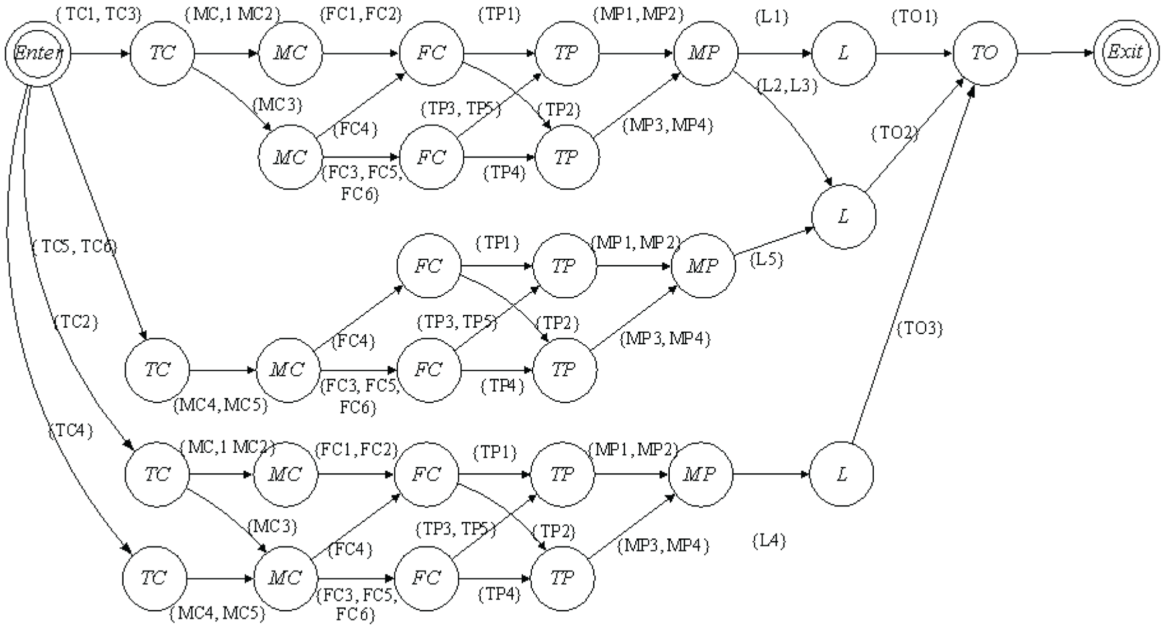


Figure 17. Model of dependencies 1 - 7



six possible values (Table 3). The total number of diversity type combinations, without consideration dependencies among them is 54,000. However, a significant part of these combinations is infeasible. Our model represents all and only feasible combinations of various diversity types. Each path through the graph represents a set of independent diversity combinations. There are no dependencies among diversity values inside each set.

The model contains 26 different paths with 374 feasible diversity combinations, as shown in Table 6.

The model allows choice of optimal design decisions with various types of diversity. The specific way of using the model depends on selected criteria. For example, if we would like to minimize cost of the design decision, the model allows easy cost calculation of each feasible di-

Table 6. Feasible combinations of diversity types

Path	TC	MC	FC	TP	MP	L	TO	Number of Feasible Combinations
1	TC1, TC3	MC1, MC3	FC1, FC3	TP1	MP1, MP2	L1	TO1	16
2	TC1, TC3	MC1, MC3	FC1, FC3	TP1	MP1, MP2	L2, L3	TO2	32
3	TC1, TC3	MC1, MC3	FC1, FC3	TP2	MP1, MP2	L1	TO1	16
4	TC1, TC3	MC1, MC3	FC1, FC3	TP2	MP3, MP4	L2, L3	TO2	32
5	TC1, TC3	MC3	FC4	TP1	MP1, MP2	L1	TO1	4
6	TC1, TC3	MC3	FC4	TP1	MP1, MP2	L2, L3	TO2	8
7	TC1, TC3	MC3	FC4	TP2	MP1, MP2	L1	TO1	4
8	TC1, TC3	MC3	FC4	TP2	MP3, MP4	L2, L3	TO2	8
9	TC1, TC3	MC3	FC3, FC5, FC6	TP3, TP5	MP1, MP2	L1	TO1	24
10	TC1, TC3	MC3	FC3, FC5, FC6	TP3, TP5	MP1, MP2	L2, L3	TO2	48
11	TC1, TC3	MC3	FC3, FC5, FC6	TP4	MP3, MP4	L1	TO1	12
12	TC1, TC3	MC3	FC3, FC5, FC6	TP4	MP3, MP4	L2, L3	TO2	24
13	TC5, TC6	MC4, MC5	FC4	TP1	MP1, MP2	L5	TO2	8
14	TC5, TC6	MC4, MC5	FC4	TP2	MP3, MP4	L5	TO2	8
15	TC5, TC6	MC4, MC5	FC3, FC5, FC6	TP3, TP5	MP1, MP2	L5	TO2	24
16	TC5, TC6	MC4, MC5	FC3, FC5, FC6	TP4	MP3, MP4	L5	TO2	24
17	TC2	MC1, MC2	FC1, FC2	TP1	MP1, MP2	L4	TO3	8
18	TC2	MC1, MC2	FC1, FC2	TP2	MP3, MP4	L4	TO3	8
19	TC2	MC3	FC4	TP1	MP1, MP2	L4	TO3	2
20	TC2	MC3	FC4	TP2	MP3, MP4	L4	TO3	2
21	TC2	MC3	FC3, FC5, FC6	TP3, TP5	MP1, MP2	L4	TO3	12
22	TC2	MC3	FC3, FC5, FC6	TP4	MP3, MP4	L4	TO3	6
23	TC4	MC4, MC5	FC4	TP1	MP1, MP2	L4	TO3	4
24	TC4	MC4, MC5	FC4	TP2	MP3, MP4	L4	TO3	4
25	TC4	MC4, MC5	FC3, FC5, FC6	TP3, TP5	MP1, MP2	L4	TO3	24
26	TC4	MC4, MC5	FC3, FC5, FC6	TP4	MP3, MP4	L4	TO3	12
Total								374

versity combination based on the costs connected with each diversity value.

Another approach is to provide a maximum level of diversity. To achieve this, we need to choose two feasible combinations from Table 6 having the maximum number of different diversity values. It is possible to use other criteria or to combine several such criteria to obtain the best diversity structure of the system.

Application of the diversity allows a decrease in the probability of common cause failure. This approach stipulates the necessity for the development of a regular procedure for generation and choice of diversity types and values. A new graphical model is presented for different variants of the diversity and can be used during the development of safety-critical systems and selection of optimal algorithms for diversity types based on a criterion of a safety-reliability-cost. The model addresses diversity types at different levels: complex electronic components (FPGA, etc.), printed circuit boards, manufacturers, specification languages, design and program languages, etc. It takes into consideration the dependencies among diversity types. The graphical model is developed using the subgraph splitting algorithm, which has been previously used for software test generation. A path through the graph represents a set of feasible diversity decisions, which are independent within a given set. All paths describe all and only feasible combinations of diversity. Based on this representation, an optimal design decision during system development can be selected.

ASSESSEMENT OF MVS SAFETY

Metric-Probabilistic Assessment of MVS Safety

General approach to metric-probabilistic assessment: The proposed approach to assessment of diversity level and MVS safety is based on the following basic procedures analysis and evaluation:

- Check-list-based analysis of applicable diversity types (CLD); initial data for the CLD analysis are I&C design and documentation, a table of diversity types (subtypes) was developed in advance; a result of the CLD analysis is a formalized structured information about used diversity types and subtypes in analyzed I&C system;
- Metric-based assessment of diversity (MAD); initial data for the MAD procedure are results of the CLD analysis and values of metrics and weight coefficients for diversity types (subtypes) used in I&C systems; a result of the MAD assessment is a value of general diversity metric;
- RBD and Markovian model-based assessment (RDM); initial data for the RDM procedure are I&C design and documentation, results of the CLD and MAD analysis; results of the RDM procedure are values of safety and dependability indicators.

General scheme of assessment based on the proposed approach is shown on Figure 18. Table of diversity types, values of metrics and weight coefficients for different options of diversity types and subtypes are formed according to results previous analysis and research.

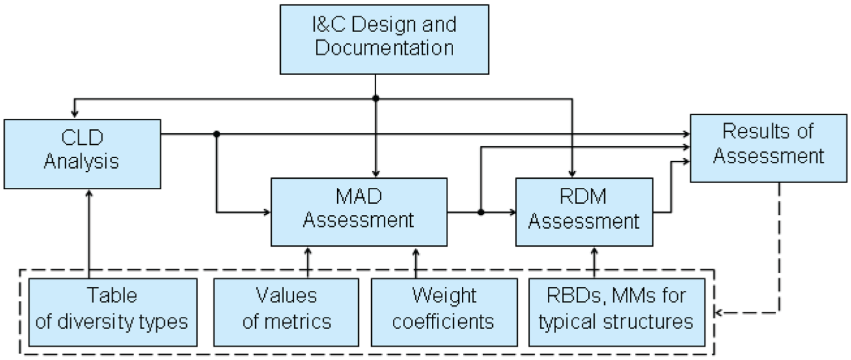
These components may be corrected after assessment of each project.

Assessment of FPGA-based MVS: The main stages and operations of the diversity analysis and MVS assessment depend on the type of the evaluated system. The following description takes into account the peculiarities of FPGA-based systems.

The first stage is a Check-list-based analysis of MVS design and documentation. This stage contains two operations:

1. Analysis of I&C specification and requirements to system, definition of system safety class; requirements to the diversity (necessary for diversity application).

Figure 18. General scheme of metric-probabilistic assessment



2. Analysis of I&C design and development process that involves activities: (a) identification of MVS types: which of the subsystems are FPGA-based and which are software and microprocessor-based; (b) identification of product diversity; for FPGA-based MVSs: manufacturer of chips; FPGA technology; FPGA families; FPGA chips, languages; tools, etc); (c) identification of process diversity types.

Results of analysis are entered in a check-list in accordance with rule Yes (if a corresponding diversity type is used in a system) / No (in opposite case) and is presented as a n-bit Boolean vector.

The second stage is a metric-based assessment of diversity:

1. Determination of metric values for different types of applied diversity, i.e. performing two activities: (a) determination of metric values (local diversity metrics μ_i for the diversity type d_i and local diversity metrics μ_{ij} for the diversity subtype d_{ij}); the metric values may be predefined; (b) correction of metric values in accordance with development and operation experience.
2. Calculation of the general diversity metric μ for a system: (a) determination (correction) of weight coefficients $\omega_i (\omega_{ij})$ of metrics (taking into account multi-diversity aspect); the sum of weight coefficients $\omega_i (\omega_{ij})$ is equal 1; (b) a convolution (additive or more complex) of metrics and a calculating value of general diversity metric $\mu = \Sigma\, \omega_i\, \Sigma\, \omega_{ij}\, \mu_{ij}$, $i = 1,\ldots, n$; $j = 1,\ldots n_i$.

Thus, result of this stage is a value of the general diversity metric μ, which is some approximation of β, and can characterize the diversity effect on CCF probability.

Assessment of software-based MVS: The metric-based assessment of software-based MVS can be made using direct metrics. General assessment technique of software-based MVS is considered by the example of two-version projects.

To assess diversity indicator β, using direct metrics, testing results of each program-version in MVS are required. Direct metrics-based assessment of diversity indicator β of two-version design has the following stages: (1) testing each program-version on the common test set; (2) error determination common for both program-versions; (3) diversity indicator determination by formula:

$$\beta = \frac{2 \cdot n_{com}}{n_1 + n_2},$$

where n_{com} – a number of errors common for both program-versions;

n_1, n_2 – a number of errors in the first and the second program-version, respectively.

In accordance with the formula, diversity indicator β changes from 0 to 1 and takes on limit values in the following cases:

$$\beta = \begin{cases} 0, \text{ if } n_{com} = 0 \\ 1, \text{ if } n_{err1} = n_{err2} \end{cases}.$$

Gain, obtained by the diversity, is $\Delta = 1 - \beta$

If all errors match in both program-versions (β=1), there will be no gain (Δ=0), because both MVS versions will operate inaccurately. If errors differ in each version (ideal case) (β=0), majority element will be able to determine different values in each channel; so, in this case there will be the largest gain (Δ=1). If diversity indicator is in the range ($0<\beta<1$), obtained gain indicates that in both versions a number of undetected errors is decreased by value (Δ*100) percentagewise.

Indirect metrics-based assessment of the diversity indicator β of two-version design has the following stages: (1) measurement of absolute values of each program-version metrics, using statistical code analyzer; (2) calculation of absolute value of remainder obtained from a pair of each program-version metrics; (3) rating absolute values of metrics obtained at stage 2; (4) determination of the diversity indicator β.

Further, values of diversity indicators, obtained by using direct and indirect metrics, should be compared to determine their correlation.

To assess proposed MVS assessment techniques two-version projects were obtained in programming languages C#, Java, C++. Only versions of initial programs with errors were assessed. Assessment results of two-version projects are presented in Table 7. Each project is a solution for one of the five tasks characterized by complexity level, where I – the lowest level of task complexity, III – the highest level (Duzhyi, V., et al, 2010).

From the table it appears:

- Diversity allows increasing quality of most projects.
- Subject diversity allows increasing project quality independently of programming language.

Table 7. Results of MVP experimental researches

Task	**Level of Complexity**	**Language**	**Number of Projects (MVP)**	**β**			**Gain by Diversity, % by MVP**
				0	**0...1**	**1**	
1	I	C#	3	2	0	1	67
		Java	91	16	61	14	85
		C++	465	99	343	23	95
2	II	C#	21	0	21	0	100
		Java	153	12	132	9	94
		C++	465	20	439	6	99
3	I	C#	45	6	38	1	98
		Java	45	0	38	7	84
		C++	435	64	323	48	89
4	II	Java	3	2	1	0	100
		C++	231	0	211	20	91
5	III	Java	3	0	3	0	100
		C++	10	4	6	0	100

- Using diversity for solving complex tasks (Levels of complexity II and III), gain turns to be larger than for simple ones (more than 90%).

Probabilistic Assessment of MVS Safety

Reliability models of MVS: Probabilistic assessment is considered in terms of Two-channel Reactor Trip System with three parallel tracks (sub-channels) of a voting logic “2-out-of-3” in each independent channel. A real system produced by RPC Radiy was taken as a basis (Kharchenko V., et al, 2008). Each of the channels of the system independently receives inputs and form outputs.

A simplified diagram of components of this system is shown in Figure 19, where $T_{i.j}$ is a track *j* in channel *i*. A reliability block diagram of Two-channel System that does not use diversity (channel diversity) is shown in Figure 20, a. This diagram does not take into account element of voting logic “1-out-of-2” (element OR in the simplest case).

The reliability index $P_{phi.j}$ determines HW reliability of the track *Ti.j* (defined, first of all, by physical failures). The reliability index P_d determines reliability defined by design faults, which may be the main source of CCF. Majority elements have reliability index P_M. Reliability of the One-version Majority Redundant System is represented by the following formula:

$$P_{1D} = \left\{1 - \left[1 - \left(3P_{ph}^2 - 2P_{ph}^3\right) P_M\right]^2\right\} P_d \qquad (8)$$

If channels are implemented in different HW and SW versions, value of P_d will consist of three components (see Figure 20, b):

$\boldsymbol{P_{dr1}}$**:** $1 - Q_{dr1}$, where Q_{dr1} – a probability of failure caused by relative design faults of the first version.

$\boldsymbol{P_{dr2}}$**:** $1 - Q_{dr2}$, where Q_{dr2} – a probability of failure caused by relative design faults of the second version.

$\boldsymbol{P_{da}}$**:** $1 - Q_{da}$, where Q_{da} – a probability of failure caused by absolute design faults (common faults of the versions).

Reliability of Diverse System is calculated by the formula:

$$P_{2D} = \left\{1 - \left[1 - \left(3P_{ph}^2 - 2P_{ph}^3\right) P_{dr} P_M\right]^2\right\} P_{da} \qquad (9)$$

We consider that $P_{dr1} = P_{dr2} = P_{dr}$ and majority elements are equally reliable.

Diversity is usually applied in such a configuration, where different channels are independently implemented with different types of diversity. However, this is not the only variant of the redundant circuit. A variant of using redundancy in tracks of one channel is shown in Figure 21.

Reliability block diagrams for the system, represented in Figure 21, are shown in Figure 22. Reliability of such system that uses one version for redundancy (Figure 5, a) can be described by the formula:

Figure 19. Simplified structure of two-channel three-track system

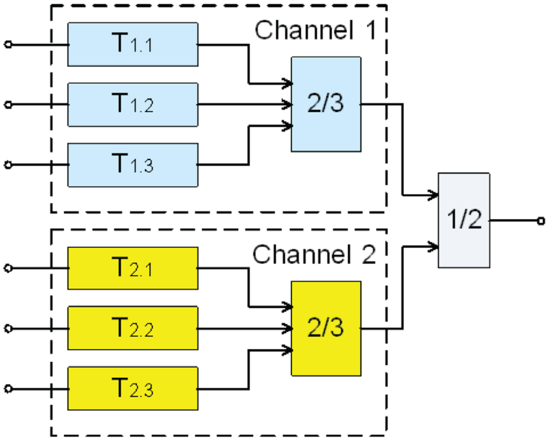


Figure 20. Reliability block diagrams of two-channel redundant system

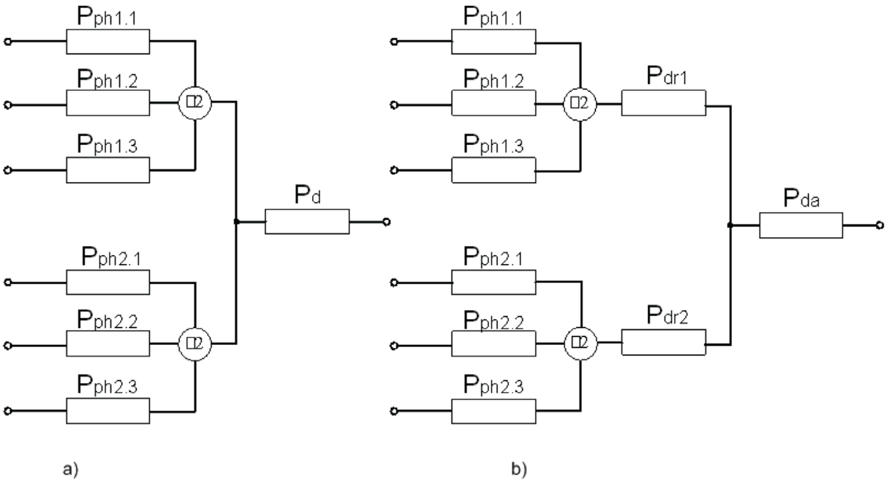
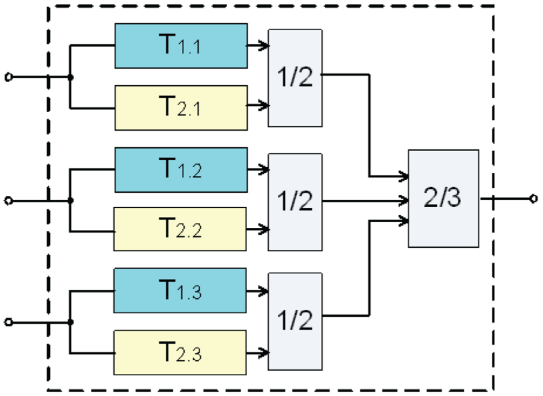


Figure 21. Simplified structure of single-channel three-track system



$$P_{1M} = \left\{ \begin{matrix} 3\left[1-\left(1-P_{ph}\right)^2\right]^2 - \\ 2\left[1-\left(1-P_{ph}\right)^2\right]^3 \end{matrix} \right\} P_M P_d \tag{10}$$

In case of using two different versions for $T_{1.i}$ and $T_{2.i}$, system has RBD, shown in Figure 22, b, and a formula for reliability calculation:

$$P_{2M} = \left\{3\left[1-\left(1-P_{ph}\right)^2\right]^2 - 2\left[1-\left(1-P_{ph}\right)^2\right]^3\right\}$$
$$P_M\left[1-\left(1-P_{dr}\right)^2\right]P_{da} \tag{11}$$

MVS reliability analysis: If we express the values of a reliability (probability of no-failure operation) through failure rates as $P = e^{-\lambda t}$, we can calculate and compare the values of reliability for certain values of λ_{ph}, λ_d, λ_M, λ_{dr}, λ_{da} and β (the fraction of absolute design faults).

Dependence of P_{1D}, P_{2D}, P_{1M} and P_{2M} (Equations 8, 9, 10 and 11)) on the time is graphically shown in Figure 23. In the calculations the following values of the failure rate were used λ_{ph}=10^{-4} 1/h, λ_d=λ_{ph}/2, λ_M=λ_{ph}/100, λ_{dr}=(1-β)×λ_d, λ_{da}=β×λ_d, where β=0,1.

Figure 24 shows how a fraction of absolute design faults (FADF is β) effects on a reliability of a single-channel divers system.

Figure 22. Reliability block diagrams of single-channel three-track redundant system

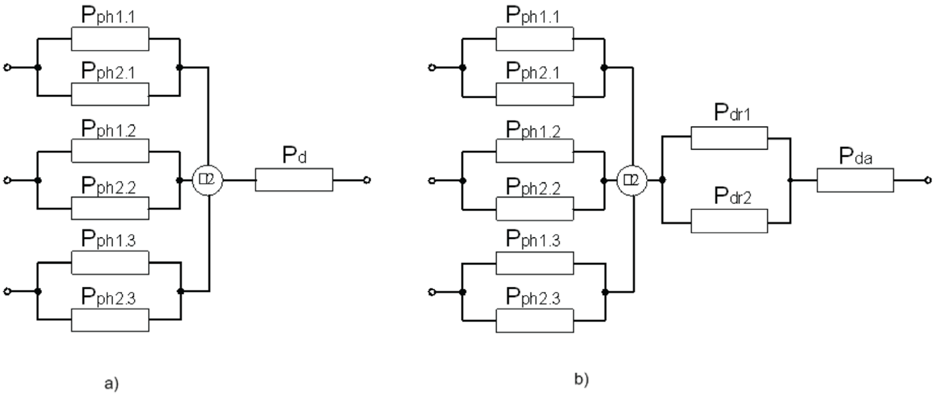


Figure 23. Dependence of P_{1D}, P_{2D}, P_{1M} and P_{2M} on the time (for systems with diversity β=0,1)

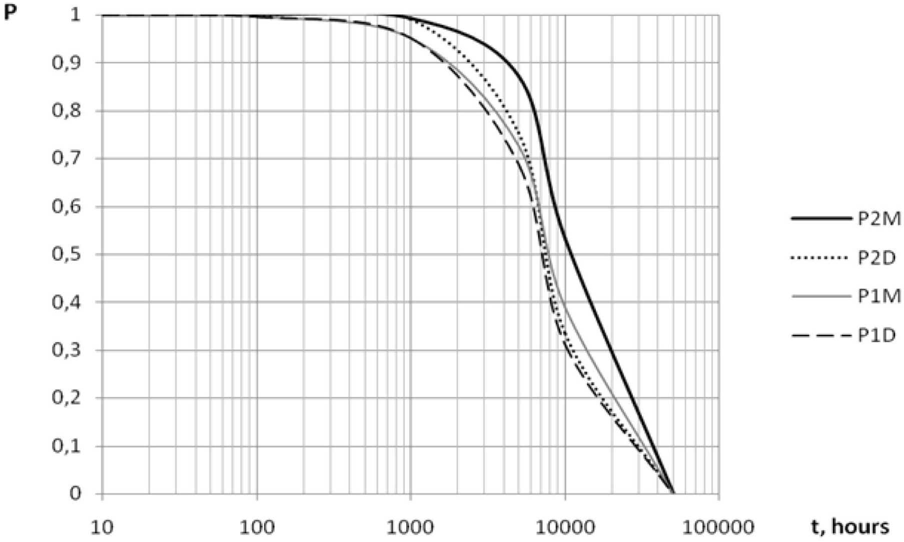


Figure 25 shows a dependence of $\Delta P_{2M\text{-}1M}$ (the difference of probabilities P_{2M} and P_{1M}) and $\Delta P_{2M\text{-}2D}$ (the difference of probabilities P_{2M} and P_{2D}) on time.

It should be noted that, although the single-channel two-version three-track redundant system has the greater effect of the use of diversity, its application in many ways violates the principle of independence. Therefore, the use of such an architecture for safety systems of nuclear power plants is complicated.

Diversity Metrics: β-Factor: To assess a probability of a common cause failure, it is necessary to calculate the metrics for different CCF vulnerabilities (Figure 26). Circles of these diagrams correspond to sets of version defects (faults) causing failure. For one-version (one-channel) system (Figure 26, a) a number of faults equals N (N = *Card F*) and any fault of set F is fatal (equivalent of CCF). In this case metric of CCF β determining relation of a number of CCFs to a total number of failures equals 1 (and $\alpha = \beta = 1$).

Figure 24. Dependence of P_{2M} on time and β

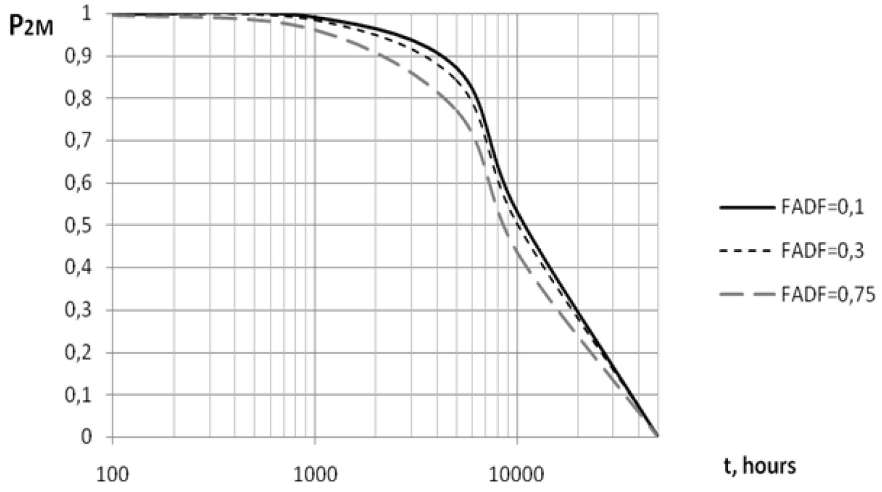
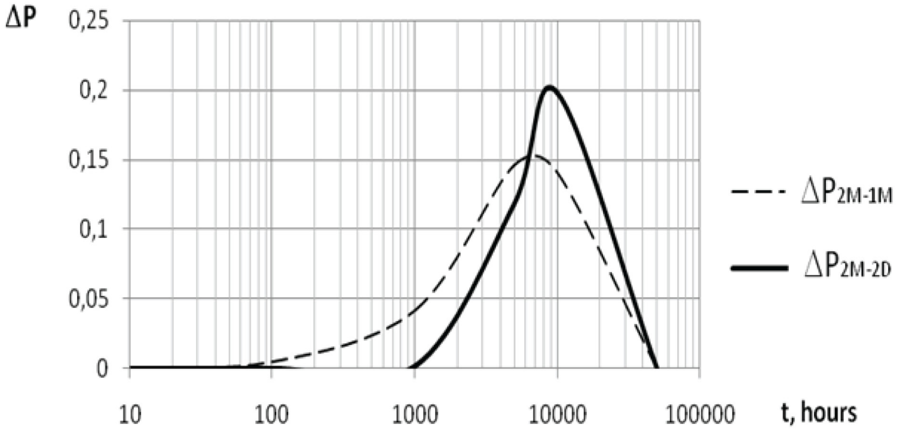


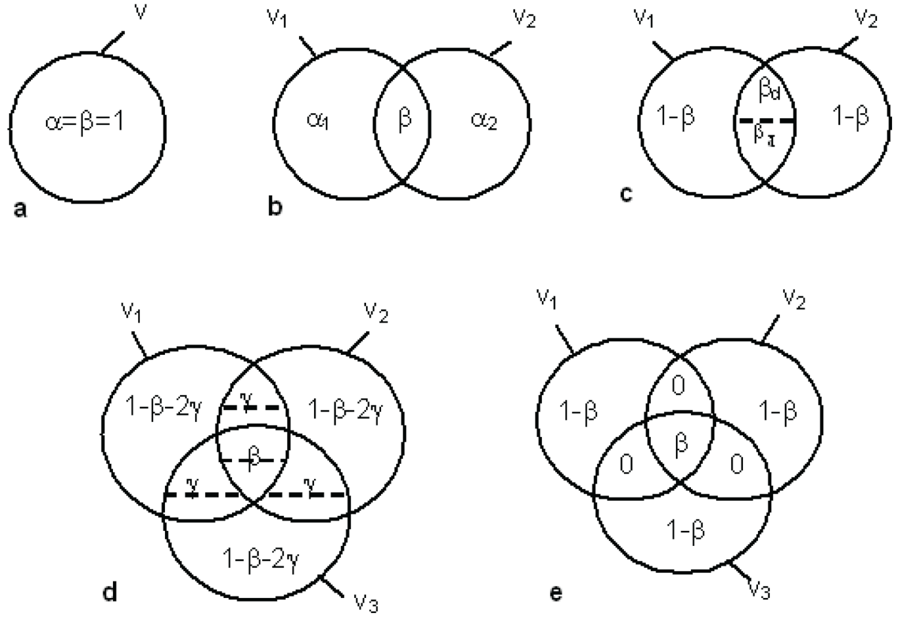
Figure 25. Dependence of ΔP_{2M-1M} and ΔP_{2M-2D} on time



For two-version system (Figure 26, b, c) CCF metric $\beta = N_{CCF} / N$, $N_{CCF} = CardF_1 \cap F_2$; the value of N may be calculated as an arithmetic mean $N = (N_1 + N_2) / 2$, $N_i = Card\ F_i$; SF metric $\alpha_i = 1 - \beta$; DCCF metric $\beta_d = N_{DCCF} / N$; UDCCF metric $\beta_{\bar{d}} = N_{UDCCF} / N$; $\beta = \beta_d + \beta_{\bar{d}}$. Besides, it is possible to use metrics of a relative number of DCCFs and UDCCFs: $\beta^*_d = \beta_d / \beta$, $\beta^*_{\bar{d}} = \beta_{\bar{d}} / \beta$.

For three-version system (Figure 26, d) $\alpha = 1 - \beta - 2\gamma$, where γ is PCCF metric (metric determining a part of CCFs of any two versions, $\gamma = 2N_{PCCF} / N$). Metrics of distinguishable and undistinguishable PSSFs are calculated by analogy β_d and $\beta_{\bar{d}}$. If $\gamma = 0$ (Figure 1,e), $\alpha = 1 - \beta$. This approach is based on the results described in (Gorbenko, A.; Kharchenko V. & Romanovsky A. 2009) and may be extended to systems, in which a set of faults is added a set of vulnerabilities attacked by an external system.

Figure 26. Diagrams of failures of one-version (a), two-version (b, c) and three-version (d, e) systems



DIVERSITY ASSESSMENT TECHNIQUES AND TOOLS

Diversity Assessment Techniques

To analyse diversity assessment techniques it is needed to describe their basic principles and procedures. Further three techniques are analysed: NUREG-A, CLB-A, GMB-A.

NUREG-A technique:

1. Features of NUREG-based assessment technique are the following:
   a. It is based on a diversity classification described in (NUREG/CR-6303, 1994, NUREG/CR-7007, 2009).
   b. It allows to fulfill metric-based assessment of two-version systems.
   c. Diversity is assessed using a value Yes or No (if Yes, there are to subvalues: INT = intentional (X), INH = inherent (i): if Altera (diversity of chip), hence Quartus (diversity of tools)).
   d. 2-level analysis procedure is used for types and subtypes of the diversity (attribute and criteria).
   e. Weight of attribute depends on rate of application of the diversity type in I&Cs.
   f. Metric is non-normalized.
   g. Acceptable value of diversity metric equals 1.0.
2. Assessment procedure consists of the following stages:
   a. An expert analyzes design and fills assessment table (X (i) or No).
   b. Diversity metric is calculated (“automatically”).
   c. An expert makes decision “accepted/not accepted.”

The described technique allows assessing level of diversity using general metrics; values of metrics are determined in advance. But this technique does not permit to calculate safety indicators of MVS safety.

CLB-A technique:

1. Features of CLB-based assessment technique are the following:
    a. It is based on a classification of diversity types described in (Kharchenko, 2011) and detailing NUREG classification.
    b. A main document is a multilevel checklist (CL) and questionnaires for assessment of diversity type application.
    c. Diversity metric is normalized [0,1].
    d. It may be used as a stage of I&C safety assessment (calculation of ?-factor, reliability and safety indicators using RBD or MM).
2. Assessment procedure consists of the following stages:
    a. Analysis of I&C specification, design and development process.
    b. Identification of MVS types, product/process diversity (according to presented CL).
    c. Determination of metric values for different n types of applied diversity (local diversity metrics μ_i for diversity type di, metrics μ_{ij} for diversity subtype dij.
    d. Determination (correction) of weight coefficients ω_i (ω_{ij}) of metrics.
    e. Calculation of the general diversity metric μ for system:

$$\mu = \Sigma\omega_i\Sigma\omega_{ij}\mu_{ij}, \; i = 1,\dots,n; \; j = 1,\dots,n_i.$$

GMB-A technique analysis: This technique is a next step of developing CLB-based one. It is additionally based on a graph model of diversity types for two-version I&C systems (number of joint nodes, k; length of a minimal version, n_{min}). It details CLB-A technique regarding evaluation of metrics and weight coefficients and takes into account features of technological and architectural aspects of applied diversity (sensors, HW, SW, design, etc.).

Besides, an acceptable value of diversity correlates with NUREG-A in this technique.

Diversity Assessment Tools

NUREG-A-based tool: NUREG-A-based tool supports corresponding technique and allows calculating the diversity metric according to attributes and criteria, values of weights (Kharchenko, 1999).

CLB-A-based tool: Tool DivA (Diversity Analysis Helper) (Kharchenko, et al., 2012; Kharchenko, et al., 2012), is based on CLB-A and has main window displays (Figure 27):

- Hierarchy (multi-level and extensible) of diversity types.
- Calculated results (weights, metrics,…)
- Options for metric calculations.

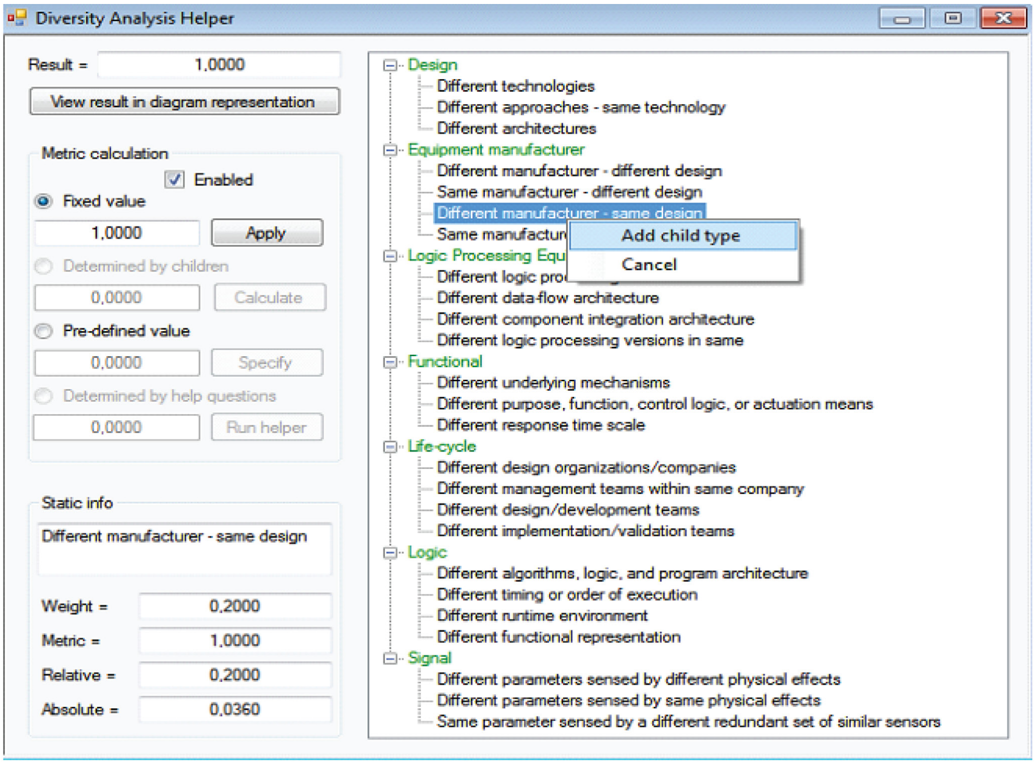
Green colours mean diversity type is included in result of calculation. Gray colours mean diversity type is disabled for managing. User can add new diversity subtype for a selected type.

There are a few metric calculation options:

- **Fixed Value:** User inputs metric manually.
- **Value determined by children:** Metric is calculated as the sum of sub-types metrics.
- **Pre-defined value:** Shows an additional window, where a user can select pre-defined metric.
- **Value determined by help questions:** Shows additional window with helper.

The special window appears after selection, for example, of “Pre-defined value” option on main window. Features of this and other options are the following:

Figure 27. Main window of the DivA tool



Diversity Analysis Helper

Result = 1,0000

Metric calculation

☑ Enabled

● Fixed value

1,0000

○ Determined by children

0,0000

○ Pre-defined value

0,0000

○ Determined by help questions

0,0000

Static info

Different manufacturer - same design

Weight = 0,2000

Metric = 1,0000

Relative = 0,2000

Absolute = 0,0360

- Design
  - Different technologies
  - Different approaches - same technology
  - Different architectures
- Equipment manufacturer
  - Different manufacturer - different design
  - Same manufacturer - different design
  - Different manufacturer - same design
  - Same manufactur
- Logic Processing Equ
  - Different logic pro
  - Different data-flow architecture
  - Different component integration architecture
  - Different logic processing versions in same
- Functional
  - Different underlying mechanisms
  - Different purpose, function, control logic, or actuation means
  - Different response time scale
- Life-cycle
  - Different design organizations/companies
  - Different management teams within same company
  - Different design/development teams
  - Different implementation/validation teams
- Logic
  - Different algorithms, logic, and program architecture
  - Different timing or order of execution
  - Different runtime environment
  - Different functional representation
- Signal
  - Different parameters sensed by different physical effects
  - Different parameters sensed by same physical effects
  - Same parameter sensed by a different redundant set of similar sensors

- Only one item can be selected.
- Dependencies between components are shown (for example, selection of Altera and Actel manufacturers causes selection of Quartus and Libero tools).
- Helper runs after selection of “Determined by use of questions” (see Figure 28) option on the main window, etc.

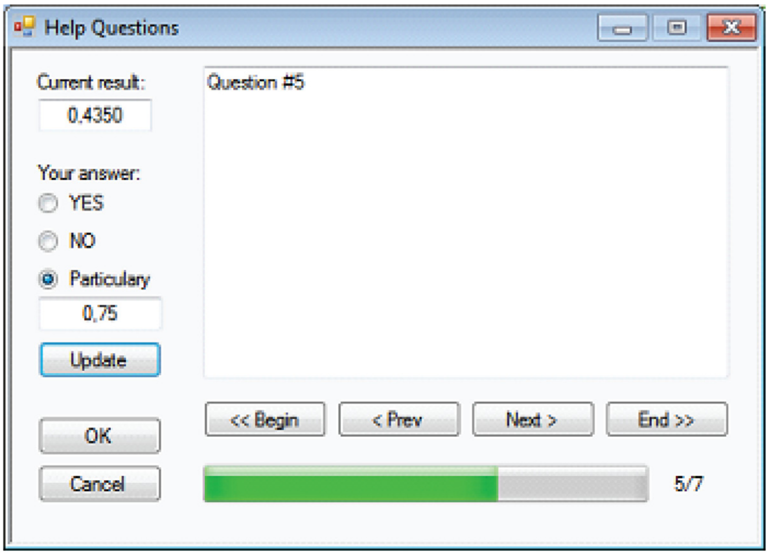
Current result represents the metric for a corresponding diversity type; user can choose answers: “YES” (answer value is considered as 1), “NO” (answer value is considered as 0), “Partially” (expected input of a answer value in the range between 0 and 1). The result is represented in the table and by coloured radial diagram. Absolute value and percentage of result are shown for each diversity type (on all levels of a diversity hierarchy).

Comparison of Diversity Assessment Techniques and Tools

Assessment of different MVSs: To analyze the selected techniques of diversity assessment, five different multi-version projects MVP-1 - MVP-5 (see Figure 29, top part) were evaluated:

- **MVP-1:** Diversity is implemented by application of different FPGA manufacturers (Altera and Actel), technologies and others.
- **MVP-1:** Diversity is implemented by application of different FPGA manufacturers (Altera and Actel), technologies (SRAM and Antifuse) and others.
- **MVP-2:** Diversity is implemented by application of different FPGA families, processes and others.

Figure 28. A special window for additional questions to calculate local diversity metrics



Help Questions

Current result:
0,4350

Your answer:
○ YES
○ NO
● Particulary
0,75

Update

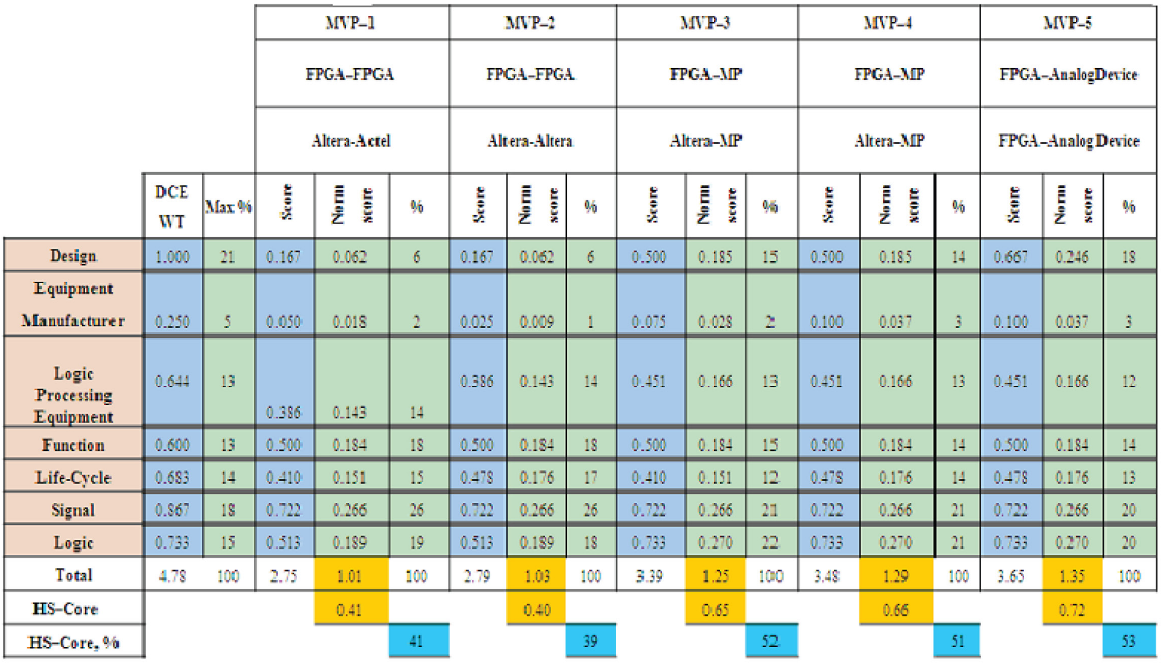
Question #5

<< Begin   < Prev   Next >   End >>

OK
Cancel

5/7

Figure 29. NUREG-A diversity assessment results for different two-version NPP I&C systems with FPGA-based subsystem



			MVP–1			MVP–2			MVP–3			MVP–4			MVP–5		
			FPGA–FPGA			FPGA–FPGA			FPGA–MP			FPGA–MP			FPGA–AnalogDevice		
			Altera-Actel			Altera-Altera			Altera–MP			Altera–MP			FPGA–Analog Device		
	DCE WT	Max %	Score	Norm score	%	Score	Norm score	%	Score	Norm score	%	Score	Norm score	%	Score	Norm score	%
Design	1.000	21	0.167	0.062	6	0.167	0.062	6	0.500	0.185	15	0.500	0.185	14	0.667	0.246	18
Equipment Manufacturer	0.250	5	0.050	0.018	2	0.025	0.009	1	0.075	0.028	2	0.100	0.037	3	0.100	0.037	3
Logic Processing Equipment	0.644	13	0.386	0.143	14	0.386	0.143	14	0.451	0.166	13	0.451	0.166	13	0.451	0.166	12
Function	0.600	13	0.500	0.184	18	0.500	0.184	18	0.500	0.184	15	0.500	0.184	14	0.500	0.184	14
Life-Cycle	0.683	14	0.410	0.151	15	0.478	0.176	17	0.410	0.151	12	0.478	0.176	14	0.478	0.176	13
Signal	0.867	18	0.722	0.266	26	0.722	0.266	26	0.722	0.266	21	0.722	0.266	21	0.722	0.266	20
Logic	0.733	15	0.513	0.189	19	0.513	0.189	18	0.733	0.270	22	0.733	0.270	21	0.733	0.270	20
Total	4.78	100	2.75	1.01	100	2.79	1.03	100	3.39	1.25	100	3.48	1.29	100	3.65	1.35	100
HS–Core				0.41			0.40			0.65			0.66			0.72	
HS–Core, %					41			39			52			51			53

- **MVP-3:** Diversity is implemented by application of different strategies (MP and FPGA) and others.
- **MVP-4:** Diversity is implemented by application of different strategies (MP and FPGA), processes and others.
- **MVP-5:** Diversity is implemented by application digital (FPGA) and analog technologies.

One of systems (main or diverse) of two-version I&C systems for analysed MVP-1, MVP-5 is based on the RadICS platform. Results of MP-1 - MP-5 assessing by use of NUREG-A and GMB-A techniques are shown in the Figures 29 – 31 (ID – total indicator of diversity calculated by use NUREG-A technique, HS-core – ID for hardware/software core of I&C system). Acceptable value of the diversity is defined by NUREG-A as ID = 1.

Besides, results of diversity assessment using these techniques for four I&C systems (PWR, DAS, AWTS which were described in (NUREG/CR-7007, 2009) and a variant of two-version RadICS-based I&C system, Radiy) are illustrated in the Figures 32 and 33 correspondingly. Results of the GMB-A diversity assessment of FPGA-based I&C are shown in the Figure 34.

Results of diversity assessment techniques comparison: Results of a comparative analysis of NUREG-A, CLB-A and GMB-A techniques are shown in the Table 8. NUREG-A technique is more general. CLB-A and GMB-A techniques are detailed to evaluate the actual diversity level of a MVS. Results of assessing a few I&C systems using the techniques are consistent (the same priority row).

ASSESSMENT OF MULTI-VERSION FPGA-BASED SYSTEMS SAFETY

General Approach to Assessment

Assessment of a diversity level and MVS safety is based on the following basic procedures analysis and evaluation:

Figure 30. Graphical illustrations of NUREG-A diversity assessment results of the MVP-1 - MVP-5

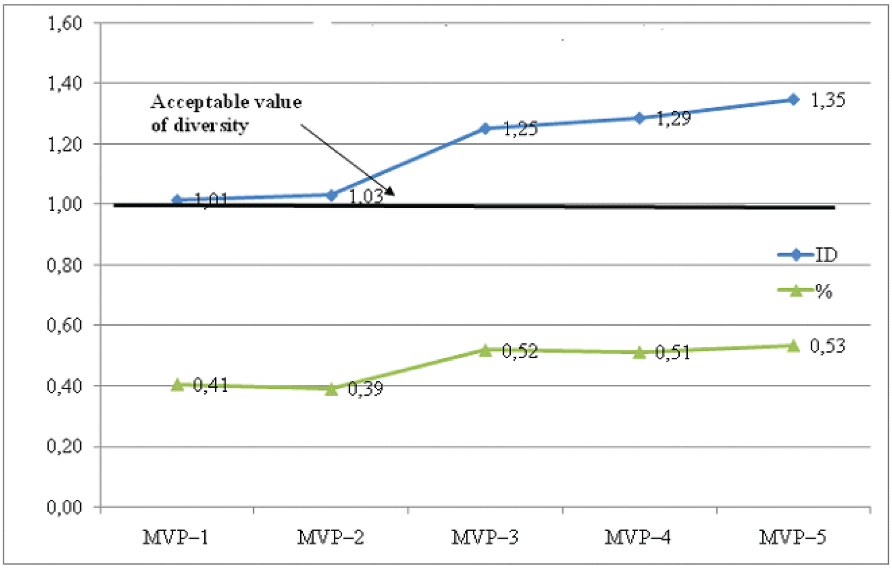


Figure 31. GMB-A diversity assessment results of the MVP-1 - MVP-5

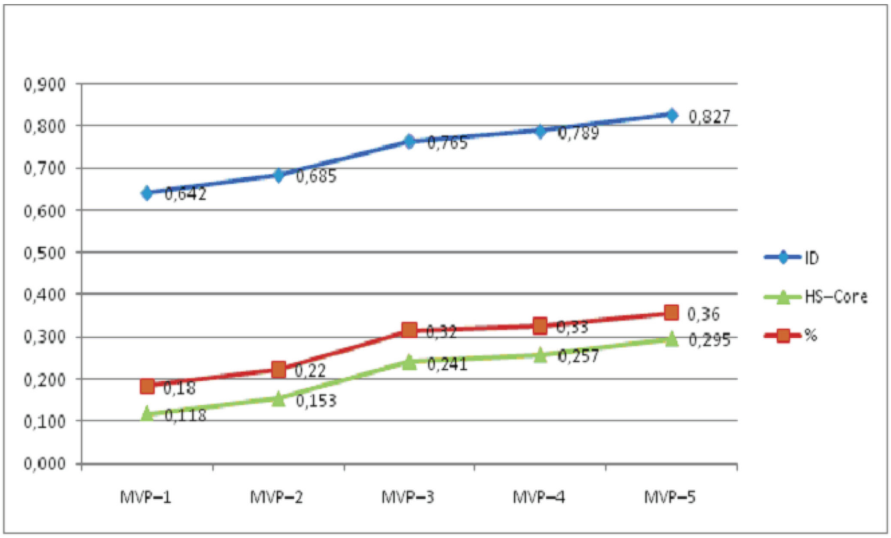
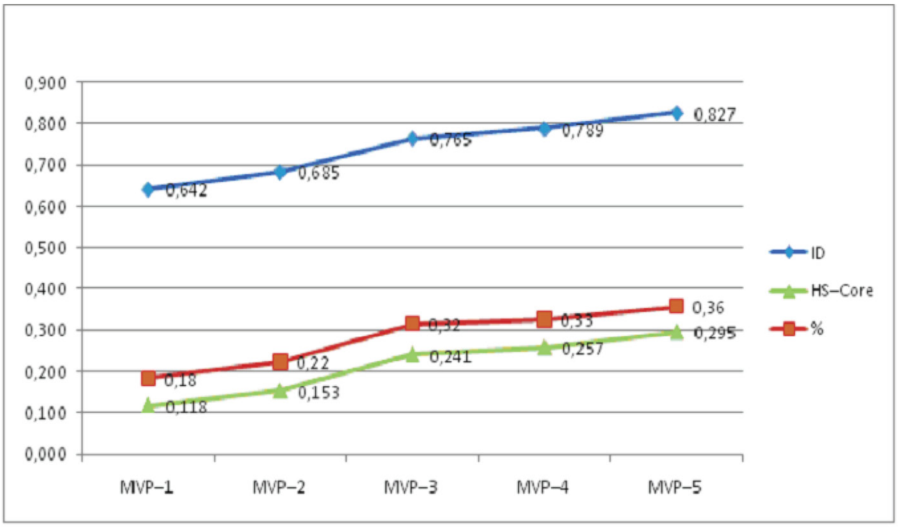


Figure 32. NUREG-A diversity assessment results of two-version I&C systems (examples taken from (NUREG/CR-7007, 2009) and RadICS-based)



- Check-list-based analysis of applicable diversity types (CLD); initial data for the CLD analysis are I&C design and documentation, a table of diversity types (subtypes) was developed in advance; a result of the CLD analysis is a formalized structured information about used diversity types and subtypes in analyzed I&C system.
- MAD; initial data for the MAD procedure are results of the CLD analysis and values of metrics and weight coefficients for diversity types (subtypes) used in I&C systems; a result of the MAD assessment is a value of general diversity metric.
- RBD and MM-based assessment taking into account results of MAD.

Figure 33. GMB-A diversity assessment results of two-version I&C systems (examples taken from (NUREG/CR-7007, 2009) and RadICS-based)

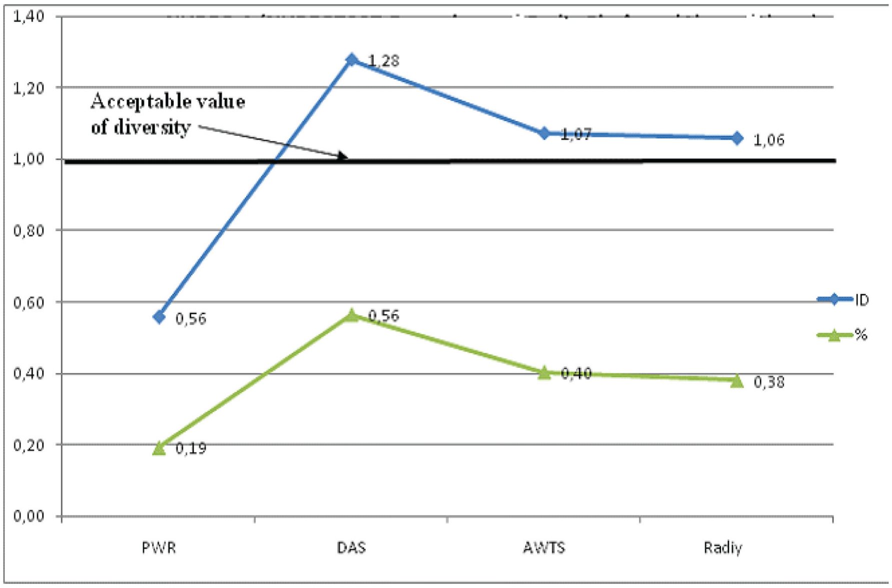
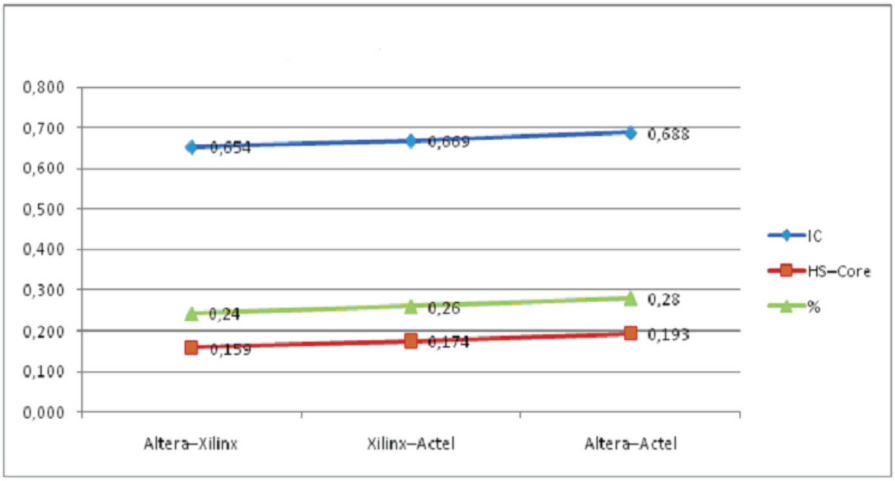


Figure 34. GMB-A diversity assessment results for FPGA-based two-version I&C systems



Stages of Assessment

The main stages and operations of diversity analysis and MVS assessment depend on the type of the evaluated system. The first stage is a Check-list-based analysis of MVS design and documentation. This stage contains two operations:

1. Analysis of I&C specification and requirements to a system, definition of system safety class; requirements to diversity (necessary for diversity application).
2. Analysis of I&C design and development process that involves activities: (a) identification of MVS types: which of the subsystems

Table 8. Results of comparative analysis of diversity assessment techniques

Technique	Diversity Classification	Number of Level	Diversity Metrics	Sensibility to Diversity Type	Tool
NUREG7007-technique	NUREG6303-based classification	Two-level hierarchy	Non-normalized	Fixed	+
CLB - technique	Extensible (in depth) NUREG7007-based classification	Multi-level	Normalized metric, may be used to calculate β factor	May be increased	+
GMB - technique	Additionally take into account feature technological and architectural aspects	Multi-level	Normalized metric, may be used to calculate β factor	May be increased	+

are FPGA-based and which are software and microprocessor-based; (b) identification of a product diversity; for FPGA-based MVSs: manufacturer of chips; FPGA technology; FPGA families; FPGA chips, languages; tools, etc); (c) identification of process diversity types.

Results of the analysis are entered in a check-list in accordance with a rule Yes (if corresponding diversity type is used in a system) / No (in opposite case) and is presented as a n-bit Boolean vector.

The second stage is a metric-based assessment of diversity. This stage contains two operations:

1. Determination of metric values for different types of applied diversity, i.e. performing two activities: (a) determination of metric values (local diversity metrics μ_i for the diversity type d_i and local diversity metrics μ_{ij} for the diversity subtype d_{ij}); the metric values may be predefined; (b) correction of metric values in accordance with development and operation experience.
2. Calculation of general diversity metric μ for a system: (a) determination (correction) of weight coefficients ω_i (ω_{ij}) of metrics (taking into account multi-diversity aspect); sum of weight coefficients ω_i (ω_{ij}) is equal 1; (b) convolution (additive or more complex) of metrics and calculating value of the general diversity metric $\mu = \Sigma\, \omega_i\, \Sigma\, \omega_{ij}\, \mu_{ij}$, $i = 1,\ldots, n$; $j = 1,\ldots n_i$.

Thus, result of this stage is a value of general diversity metric μ, which is some approximation of β, and can characterize the diversity effect on CCF probability.

The third stage is a probabilistic RBD- or MM-based (RDM) assessment of MVS reliability and safety. Initial data for the RDM procedure are I&C design and documentation, results of the CLD and MAD analysis; results of the RDM procedure are values of safety and dependability indicators. Detailed description of the RDM procedure is given in (Kharchenko et al., 2004).

IMPLEMENTATION OF FPGA-BASED SAFETY-CRITICAL NPP I&CS: UKRAINIAN EXPERIENCE

General Description of the FPGA-Based RADIY Platform

The platform RADIY produced by RPC Radiy is an example of a dependable and scalable FPGA-based I&C platform ensuring possibility of development of multi-version systems. Dependability assurance feature of the I&C platform RADIY is a multi-diversity implementation through the following diversity types: equipment diversity is provided by different electronic components, different programmable components (FPGAs and microcontrollers) and different schemes of units; software diversity is provided by different programming languages and different tools for development and verification; life cycle (human) diversity is provided by different teams of developers.

Scalability of I&C platform RADIY permits to produce different types of safety-critical systems without essential changing of hardware and software components. The I&C platform RADIY provides the following types of scalability: scalability of system functions types, volume and peculiarities by changing quantity and quality of sensors, actuators, input/output signals and control algorithms; scalability of dependability (safety integrity) by changing a number of redundant channel, tiers, diagnostic and reconfiguration procedures; scalability of diversity by changing types, depth and criteria of diversity choice.

The FPGA-based I&C RADIY platform comprises both upper and lower levels (Kharchenko&Sklyar, 2008). The upper level has been created on purchased IBM-compatible industrial workstations. The software for the upper level RADIY platform was developed by RPC Radiy and is loaded on the workstations. The functions of the upper level workstations are the following: receipt of the process and diagnostic information; creation of a man-machine interface in the Control Room; display of process information on each of the control algorithms relating to a control action executed by I&C system components; display of diagnostic information on failures of I&C system components; registration, archiving and visualization of process and diagnostic information.

The lower level of the RADIY platform consists of standard cabinets including standard functional modules blocks). The RADIY platform comprises the following standard cabinets (Bakmach et al., 2009):

- Normalizing Converters Cabinets performs inputting and processing of discrete and analog signals as well as feeding sensors.
- Signal Forming Cabinets performs inputting and processing of discrete and analog signals, processing of control algorithms, and formation of output control signals.
- Cross Output Cabinets receives signals from three control channels (signal formation cabinets) and forms output signals by “two out of three” mode.
- Remote Control Cabinets controls 24 actuators on the basis of Control Room signals, automatic adjustment signals and interlocks from signal formation cabinets.
- Signalling Cabinets forms control signals for process annunciation panel at Control Room and others.

The platform includes the following main modules: chassis and backplanes; power supply modules; analog input modules; normalizing converter modules, thermocouples; normalizing converter modules, resistive temperature detector; discrete input modules; discrete information input modules, pulse; potential signals input modules, high voltage; protection signal forming modules (logic modules); analog output modules, voltage; analog output modules, current; discrete output modules; potential signal output modules; solid-state output modules; relay output modules; actuator control modules; fiber optic communication modules; system diagnostic modules; fan cooling modules etc.

The latest RPC Radiy innovation is the FPGA-based Digital Instrumentation and Control Platform RadICS. This is a new generation product, designed in 2011 on the basis of an earlier RADIY platform having more than 10 years of experience in a platform design, manufacturing, operation, and maintenance. The RadICS platform provides IEC 61508:2010 SIL 3 architecture in an individual chassis, fast response time (less than 5 ms) and a comprehensive set of functional modules.

Opportunities of the RADIY Platform

Application of the RADIY platform with the use of FPGA technology provides the following opportunities:

- To implement control and other safety-critical functions in the form of FPGA with implemented electronic design, without software.
- To use software only for diagnostics, archiving, signal processing, data reception and transfer between I&C systems components; failures of those functions do not affect execution of basic I&C systems control functions, and an operation system is not applied at I&C systems lower levels.
- To process parallel of all control algorithms within one cycle, thus ensuring high performance of the system (for instance, a processing cycle of Reactor Trip System is 20 ms) and proven determined temporal characteristics.
- To develop the software-hardware platform in such a way that it becomes a universal interface to create I&C systems for any type of reactors.
- To assure high reliability and availability due to the application of industrial components as well as using the principles of redundancy, independency, single failure criterion, and diversity.
- To modify the I&C system after commissioning in a quite simple manner, including algorithm alterations, without any interference in I&C systems' hardware structure.
- To reduce by more than 10 times the number of contact and terminal connections, which cause many operational failures of equipment on account of the wide use of integrated solutions and fiber optic communication lines, etc.

Licensing of the RADIY Platform

The RADIY platform has been licensed for NPP application in Ukraine and in Bulgaria. The main idea for licensing FPGA-based NPP I&C systems lays in consideration of FPGA-chip as hardware and FPGA electronic design as a special kind of software with specific development and verification stages (Siora et al., 2009).

Qualification tests of FPGA-based hardware in accordance with International Electrotechnical Commission (IEC) standard requirements include: radiation exposure withstand qualification; environmental (climatic) qualification; seismic and mechanical impacts qualification; electromagnetic compatibility qualification. Results of qualification tests confirmed FPGA-based hardware compliance with IEC safety requirements.

FPGA electronic design has a V-shape life cycle in accordance with requirements of standard IEC 62566 "NPP – I&C important to safety – Selection and use of complex electronic components for systems performing category A functions."

The safety assessments have been conducted by Ukrainian State Scientific Technical Centre on Nuclear and Radiation Safety (SSTC NRS), which is the supporting organization of Ukrainian Regulatory Authority. Experts of SSTC NRS have considerable experience in the area of FPGA-based systems safety assessment, as they have performed reviews of all thirty three FPGA-based safety systems supplied to Ukrainian NPP units since 2003.

Implementation of the RADIY Platform-Based I&Cs in NPPs

The RADIY platform has been applied to the following NPP I&Cs systems, which perform reactor control and protection functions: Reactor Trip Systems (RTS); these I&Cs were developed as two-version systems consisting of two triple module redundant subsystems; It should be noted that this list is not concluded because of an universality of Radiy Platform. PRC Radiy has the ability to build different digital I&C systems for reactors of any type. The example of two-channel RTS is shown at Figure 35.

Both channels implemented on Radiy Platform. Reactor Power Control and Limitation System; Engineering Safety Features Actuation System (ESFAS); Control Rods Actuation System; Automatic Regulation, Monitoring, Control, and Protection System for Research Reactors; these I&Cs were developed as one-version systems consisting of triple module redundant subsystems.

The first commissioning of the RADIY platform was done in 2003 for Ukrainian NPP unit Zaporozhe-1. In seven years since that time, more than 80 applications of RPC Radiy systems have been installed in 17 nuclear power units in Ukraine and Bulgaria. These systems are commissioned in pressurized water reactor (PWR) plants known as “WWER” reactors developed by the former Soviet Union. WWER reactors are used in Armenia, Bulgaria, China, Czech Republic, Finland, Hungary, India, Iran, Russia, Slovakia, and Ukraine.

The largest project implemented by RPC Radiy is the modernization of six ESFASs for Bulgarian NPP Kozloduy (three ESFASs for Kozloduy-Unit 5 and three ESFASs for Kozloduy-Unit 6).

RADIY RTS DIVERSITY ASSESSMENT

Radiy RTS Diversity Assessment Based on General Approach

RADIY Platform can be used for building whole multi-channel systems as well as for building one (primary or diverse) channel of I&C System. For cases using the platform in several channels of a system, diverse solutions should be used and appropriate diversity assessment have to be performed.

The following example shows the results of assessment for two variants of RTS. Both systems are two-channel and have diverse channels with primary channel based on Altera FPGA. The first variant diverse channel is based on Actel FPGA (see Table 9). The second variant uses FPGA produced by Xilinx in the diverse channel (see

Figure 35. Radiy platform based Reactor Trip System with primary and diverse channels

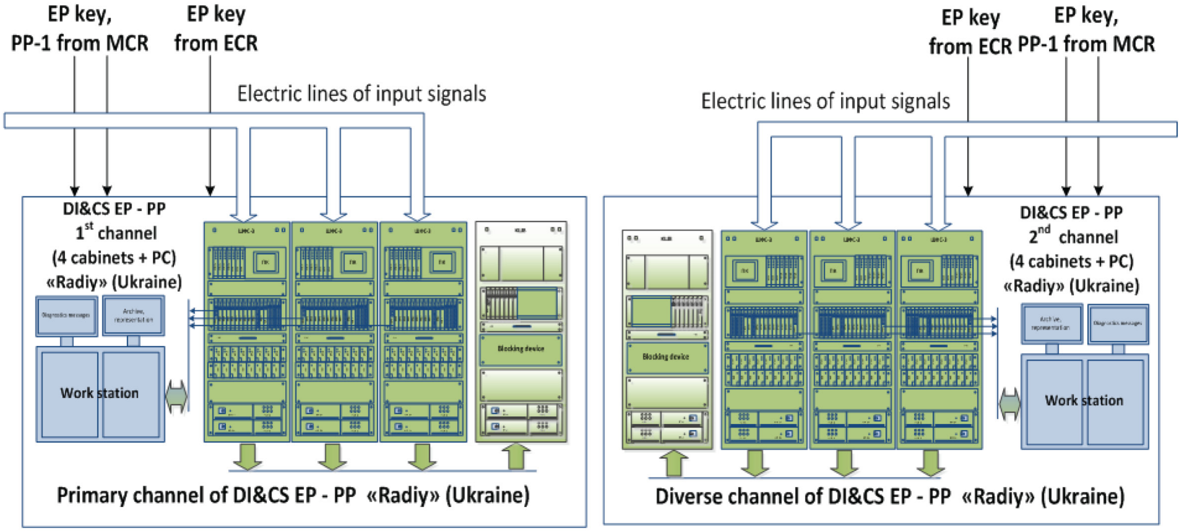

EP key, PP-1 from MCR
EP key from ECR
Electric lines of input signals
DI&CS EP - PP 1st channel (4 cabinets + PC) «Radiy» (Ukraine)
Diagnostics messages
Archive, representation
Work station
Blocking device
Primary channel of DI&CS EP - PP «Radiy» (Ukraine)
EP key from ECR
EP key, PP-1 from MCR
Electric lines of input signals
DI&CS EP - PP 2nd channel (4 cabinets + PC) «Radiy» (Ukraine)
Archive, representation
Diagnostics messages
Work station
Blocking device
Diverse channel of DI&CS EP - PP «Radiy» (Ukraine)

Table 10). Data in Tables 9 and 10 shows that using FPGA chips from different manufacturers allows obtaining the value of the general diversity metric more than 0.7. Increasing this value is possible primarily by increasing the independence of the processes and enhancement of the diversity of languages and models.

Described models of multi-version systems and multi-version technologies (life cycle) may support selecting of cost-effective technique and optimal architecture according to requirements to diversity, safety, reliability and limitation of applied technologies. These theoretical issues were used on development of FPGA-based I&C RADIY

Table 9. Assessment of the first variant of two-channel system (Altera and Actel FPGA)

Diversity Types		Result of Analysis		Assessment Results		
		Yes/ No	Implementation	Local Metric	Ratio	Weighting Coefficient
Diversity of programmable components (A)	Diversity of manufacturers of FPGA (A1)	Yes	Altera vs. Actel	0.8	0.25	0.25
	Diversity of technologies of FPGA producing (A2)	Yes	SRAM vs. Antifuse	1	0.4	
	Diversity of FPGA families (A3)	Yes	Cyclone vs. ProASIC (based on A1)	1	0.25	
	Diversity of FPGA from the same family (A4)	Yes	different families (based on A1)	1	0.1	
Diversity of printed circuit boards (PCBs) (B)	Diversity of PCB development technologies and manufacturers	Yes	Different manufacturers but the same technology	0.5	1	0.15
Diversity of CASE-tools (C)	Diversity of CASE-tools developers (C1)	Yes	Altera vs. Actel	1	0.5	0.15
	Diversity of CASE-tools (C2)	Yes	Quartus II vs. Libero (based on C1)	1	0.3	
	Diversity of CASE-tools configurations (C3)	Yes	Different tools for design but the same for verification	0.7	0.2	
Diversity of languages of FPGA projects development (D)	Diversity of language kinds (D1)	Yes	Graphic Notation and Hardware Description Language are used	0.5	0.4	0.15
	Diversity of hardware description languages (D2)	Yes	VHDL vs. Verilog	0.8	0.6	
Diversity of specification presentation (E)	Diversity of FPGA initial specification languages (E1)	No	The same language	0	0.5	0.1
	Diversity of FPGA specification models (E2)	Yes	B&HDL used for Altera	0.8	0.5	
Diversity of processes (P)	Diversity of development processes (P1)	Yes	Different teams	0.7	0.5	0.2
	Diversity of verification processes (P2)	Yes	Different departments	0.85	0.3	
	Diversity of maintenance (P3)	Yes	Different teams	0.7	0.2	
Overall assessment (general diversity metric)						0.74

platform. Main peculiarities of the platform are realization of control and other safety-related functions without software and ensuring dependability- and diversity-scalable decisions of safety-critical I&C. Experience of RPC Radiy has proved effectiveness of these decisions.

Cost–Effective Approach to RTS Diversity Assessment under Uncertainties

Nowadays, the uncertainties, associated with an alternative RTS diversity assessment, create a demand for the methods to make possible the translation, to a mathematical language, of the

Table 10. Assessment of the second variant of two-channel system (Altera and Xilinx FPGA)

Diversity types		Result of analysis		Assessment results		
		Yes/No	**Implementation**	**Local metric**	**Ratio**	**Weighting coefficient**
Diversity of programmable components (A)	Diversity of manufacturers of FPGA (A1)	Yes	Altera vs. Xilinx	0.8	0.25	0.25
	Diversity of technologies of FPGA producing (A2)	No	SRAM	0	0.4	
	Diversity of FPGA families (A3)	Yes	Cyclone vs. Virtex (based on A1)	1	0.25	
	Diversity of FPGA from the same family (A4)	Yes	different families (based on A1)	1	0.1	
Diversity of printed circuit boards (PCBs) (B)	Diversity of PCB development technologies and manufacturers	Yes	Different manufacturers and technologies	1	1	0.15
Diversity of CASE-tools (C)	Diversity of CASE-tools developers (C1)	Yes	Altera vs. Xilinx	1	0.5	0.15
	Diversity of CASE-tools (C2)	Yes	Quartus II vs. ISE (based on C1)	1	0.3	
	Diversity of CASE-tools configurations (C3)	Yes	Different tools for design but the same for verification	0.7	0.2	
Diversity of languages of FPGA projects development (D)	Diversity of language kinds (D1)	Yes	Graphic Notation and Hardware Description Language are used	0.5	0.4	0.15
	Diversity of hardware description languages (D2)	Yes	VHDL vs. Verilog	0.8	0.6	
Diversity of specification presentation (E)	Diversity of FPGA initial specification languages (E1)	No	The same language	0	0.5	0.1
	Diversity of FPGA specification models (E2)	Yes	B&HDL used for Altera	0.8	0.5	
Diversity of processes (P)	Diversity of development processes (P1)	Yes	Different teams	0.7	0.5	0.2
	Diversity of verification processes (P2)	Yes	Different departments	0.85	0.3	
	Diversity of maintenance (P3)	Yes	Different teams	0.7	0.2	
Overall assessment (general diversity metric)						0.72

intangible values and human experience, improving the available resources in the decision making process in this complicated area.

Usually, in a quantitative setting, the information is expressed by means of numerical values. However, when we work in a qualitative setting, that is, with a vague or imprecise knowledge, the information cannot be estimated with an exact numerical value. In that case, a more realistic approach may be to use linguistic assessments instead of numerical values, that is, to suppose that the variables, which participate in the problem area, are assessed by means of linguistic terms (Zadeh L. 1999, Mendel, 2002).This approach is appropriate for a lot of problems, since it allows a representation of the information in a more direct and adequate form if we are unable to express it with precision.

A linguistic variable differs from a numerical one in that its values are not numbers, but words or sentences in a natural or artificial language. Since words, in general, are less precise than numbers, the concept of a linguistic variable serves the purpose of providing a means of approximated characterization of phenomena, which are too complex or too ill-defined to be amenable to their description in conventional quantitative terms.

In fact, considering the approach suggested in (NUREG/CR-7007, 2009; NUREG/CR-6003, 1994), it is often difficult to determine the precise values of diversity attributes' weights and rank of all alternatives on diversity criteria. We need to evaluate all appropriate experience of applications of different diversity approaches in all industrial area, take into account all relevant statistics of I&C failures caused by CCFs etc. A part of this information is often represented as linguistic information, being the expert's subjective opinions. The transformation and formalization of this linguistic information into precise form without application of special methods is characterized by loss of important information. This is another aspect, which increases the difficulties of the I&C diversity assessment.

At the initial stage of selection of secondary (primary) RTS it is more convenient approach for the experts to compare the possible alternatives of primary (secondary) RTS and express their preferences using the natural language expressions.

The experts have to deal with portion of a qualitative information stipulated by several types of the following uncertainties:

- Uncertainties caused by lack of a sufficient and objective information on RTSs, which could be considered as an alternative for given RTS. The lack of required information is stipulated by policies of some I&C company-manufacturer to conceal the part of information related to its possible shortages and defects. In addition, a part of information on RTS features is confidential and not available for objective expert assessment.
- Strategic Uncertainties caused by dependencies on activities of other subjects involved (directly or indirectly) in the process of selection of alternative RTS (partners, suppliers etc.)
- Uncertainties caused by application of an imprecise information (different system parameters) expressed in natural language (for example the linguistic nature of some diversity attributes).

On the one hand, it is possible to neglect all these uncertainties and use deterministic approaches for selection of the most diverse I&C system for a given one. But on the other hand, some of important information might be lost.

We suggest using fuzzy metrics, derived from application of Computing, with words (CW) methodology to form the initial subset of possible alternatives and determine the most diverse I&C system under uncertainties.

Diversity strategies description: According to (NUREG/CR-7007, 2009; NUREG/CR-6003, 1994) the rational choice of a pair of primary and secondary RTS could be named as diversity strategies. Both of (NUREG/CR-7007, 2009; NUREG/CR-6003, 1994) describe three types of diversity strategies.

Strategy S_1 focuses on the use of fundamentally diverse technologies as the basis for RTS diverse systems, redundancies, or subsystems. In this case, the primary RTS is built on an analog (digital) technology, and the diverse RTS is based on a digital (analog) platform. This choice of technology *inherently* contributes notable equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities.

Intentional application of life-cycle and equipment manufacturer diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted.

Strategy S_2 involves the use of distinctly different technology approaches as the basis for diverse RTS, redundancies, or subsystems. In other words, this approach presumes using some variations inside either digital or analog technologies. In this case, the primary RTS is built on general-purpose microprocessors (MC), and the diverse RTS is based on, for example, FPGA platform.

This choice of technology inherently contributes some measure of equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities. Intentional application of a logic processing equipment, life-cycle, and equipment manufacturer diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted.

Strategy S_3 represents the use of architectural variations within a technology as the basis for diverse systems, redundancies, or subsystems. In this case, the primary RTS is built on static random access memory (SRAM)-based FPGA, and the diverse RTS is based on, for example, on Flash –based FPGA platform.

This choice of technology inherently contributes some limited degree of equipment manufacturer, life-cycle, and logic diversities. Intentional application of equipment manufacturer, logic processing equipment, life-cycle, and logic diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted.

Considering the system approach to strategies formulation and representation, represented in NUREGs 6303, 7707 two additional strategies S_4 and S_5 are introduced in this section.

Strategy S_4 represents the variations inside of one SRAM (Flash) FPGA technologies. One family of SRAM (Flash) FPGA is used for the primary RTS, and second (third) family of SRAM (Flash) FPGA is used for secondary RTS. For example, the primary RTS is based on application of Arria family FPGA (Altera), and the secondary RTS is based on application of Stratix family FPGA (Altera).

Strategy S_5 represents the variation inside of SRAM (Flash) FPGA family. The application of this technology supposes using the representatives from one family to provide diversity for both secondary and primary RTS. For example, the primary RTS is based on application the Stratix II FPGA, and the secondary RTS is based on application of Stratix III FPGA.

It is apparently that the lower layer of hierarchy the less diversity for I&C provided. Each strategy is characterized by the set of possible alternatives (secondary RTS) available to provide the diversity between the primary and secondary RTS. The bigger index of strategy the more possible alternatives are available.

The choice of strategies is stipulated by the existence of some restrictions, which could limit the set of possible alternatives for the secondary RTS. The S_1 strategy represents the policy of absence of any restrictions (financial, organizational, political etc) related to the choice of the secondary RTS.

The S_2 strategy is characterized by the freedom "inside" of digital technology. Any of FPGA –based RTS could be chosen as primary RTS and any of MC –based RTS could be selected as a secondary one.

The S_3 strategy is characterized by some freedom "inside" of FPGA technology. In this case, there are no restrictions for selection any FPGA-based RTS either SRAM or Flash.

The S_4 strategy is characterized by some freedom "inside" of FPGA SRAM (Flash) technology. In this case, the second RTS could be selected from FPGA SRAM (Flash) families.

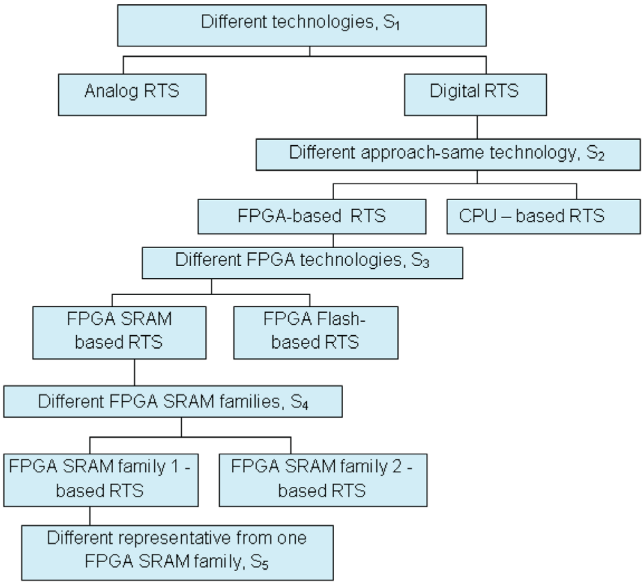
The S_5 strategy is characterized by freedom "inside" of one family of FPGA SRAM (Flash) technology. In this case, the second RTS could be selected from one of family of FPGA SRAM (Flash) families.

Generally, each S_i diversity strategy includes the subset of diversity strategies S_{ij}, where j – a number of possible alternatives classified as a type of S_i strategy. For example, different types of S_3 might be the following strategies: S_{31} – the primary RTS – FPGA SRAM – based RTS (Stratix IV (E,GX,GT)) and the secondary RTS – FPGA FLASH-based RTS (XC3000), S_{32} – the primary RTS – FPGA SRAM – based RTS (Stratix IV (E,GX,GT)) and the secondary RTS – FPGA Flash-based RTS (XC4000), S_{33} – the primary RTS – FPGA SRAM – based RTS (Stratix IV (E,GX,GT)) and the secondary RTS – FPGA Flash-based RTS (Virtex), etc.

The hierarchy of diversity strategies is shown on Figure 36.

The stages of RTS diversity assessment: The linguistic approach for selection of the most diverse RTS (Zadeh, 1999) deals with qualitative aspects that are represented in qualitative terms by means of linguistic variables. When a problem is solved using linguistic information, it implies the need for computing with the words (CW) (Zadeh, 1999). Since CW deals with words or sentences defined in a natural or artificial language instead of numbers, it emulates human cognitive processes to improve solving processes of problems dealing with uncertainty. Consequently, CW has been applied as a computational basis to linguistic decision making, because it provides tools close to human beings reasoning processes related to decision making, which improve the resolution of decision making under uncertainty as linguistic decision making. CW is an approximate technique in its essence, which represents qualitative

Figure 36. The hierarchy of diversity strategies


Different technologies, S_1
Analog RTS
Digital RTS
Different approach-same technology, S_2
FPGA-based RTS
CPU – based RTS
Different FPGA technologies, S_3
FPGA SRAM based RTS
FPGA Flash-based RTS
Different FPGA SRAM families, S_4
FPGA SRAM family 1 - based RTS
FPGA SRAM family 2 - based RTS
Different representative from one FPGA SRAM family, S_5

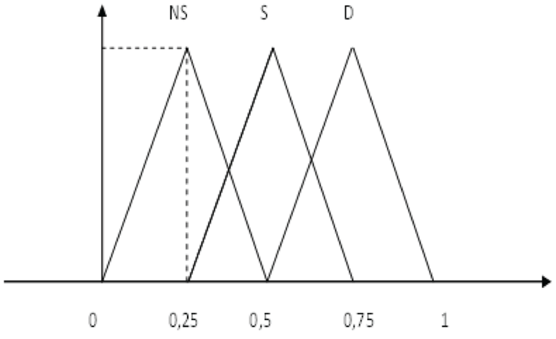
aspects as linguistic values by means of linguistic variables, that is, variables, whose values are not numbers but words or sentences in a natural or artificial language.

To compare the secondary and primary RTS, using the diversity criteria and evaluate the similarity (difference), expert should take into consideration the compelling evidence (i.e., some adequate combinations of thorough testing, substantial usage history for a comparable application under very similar demands and conditions, extensive formal proofs, detailed hazard/threat analysis, etc.). Based on these evidences experts evaluate the difference (similarity) between the primary RTS and secondary RTS for each diversity strategy using the linguistic terms: SAME (S), NEARLY SAME (NS), DIFFERENT (D).

The stage of cost – effective approach to selection of diverse NPP RTS consists of the following stages.

The formation of diversity strategies set: When the primary RTS has been already determined, and a set of possible alternatives for the secondary RTS has also been established, it is suggested to classify the type of a diversity strategy according to the hierarchy of diversity strategies shown in Figure 37. When the type of a diversity strategy is determined, it is suggested to use the set of diversity criteria predefined in (NUREG/CR-7007, 2009; NUREG/CR-6003, 1994). These diversity criteria are used to complete the comparison matrixes. These comparison matrixes are chosen according to strategies used to provide the required diversity. The example for evaluation of a subset of the diversity strategy S_3 is shown in the Table 11. In this case the primary RTS is FPGA Flash – based RTS (A3PE1500 from ProASIC 3/E family, Actel).

Figure 37. A set of terms with its semantic



The possible alternatives for the second RTS are FPGA Flash (SRAM) – based RTS. The following diversity strategies are considered:

S_{31}: The primary RTS is Flash – based RTS (A3PE1500, ProASIC 3/E family, Actel) and the secondary RTS – FPGA SRAM – based RTS (EP1SGX40G, Cyclone IV GX family, Altera).

S_{32}: The primary RTS is Flash – based RTS (A3PE1500, ProASIC 3/E family, Actel) and the secondary RTS – FPGA Antifuse – based RTS (AX2000, Axcelerator family, Actel).

S_{33}: The primary RTS is Flash – based RTS (A3PE1500, ProASIC 3/E family, Actel) and the secondary RTS – FPGA Antifuse – based RTS (QL904M, QuickMIPS family, QuickLogic).

The diversity strategies set's expertise: During this stage experts are supposed to fill the comparison matrixes to evaluate the similarities (differences) between the primary RTS and each of possible alternatives of secondary ones. The expert is also required to assign the weight of each criterion. Generally, the weight might be evaluated on various scales. The criterion's weight might be expressed either as linguistic value (Low, Medium, High) or any numerical values from [0, 1]. The more weight the more criterion influence on diversity RTS. For sake of simplicity the weight of criterion is presented as scalar value.

Table 11 represents the example of diversity assessment for the set of alternative strategies S_3 (different FPGA technologies) and corresponding set of diversity criteria, which could be applicable for diversity evaluation.

Table 11. The example of comparison matrix for strategies S3 (different FPGA technologies)

Diversity Criterion	W_k, Weight of Diversity Criterion	Alternative RTSs		
		Strategy S_{31}, $FPGA_1$	Strategy S_{32}, $FPGA_2$	Strategy S_{33} $FPGA_3$
Design				
Technologies	0,21	S	D	D
Approach (for the same technology)	0,19	S	NS	NS
Architecture	0,6	D	S	D
Equipment Manufacturer				
Design (for different Manufacturer)	0,5	S	D	D
Design (for the same Manufacturer)	0,5	D	D	NS
Logic Processing equipment				
Logic Processing Architecture	0,3	D	D	S
Component integration Architecture	0,7	S	D	NS
Functional				
Purpose, function, control logic, or actuation means	1	S	D	D
Life-cycle				
Design organizations/companies	0,24	S	D	NS
Design/development teams	0,36	D	NS	NS
Implementation/validation teams	0,4	S		D
Logic				
Algorithms, logic, program architecture	0,33	D	D	D
Runtime environment	0,47	D	NS	D
Functional representation	0,2	D	S	S
Signal				
Parameters sensed	0,6	D	NS	S
Physical effects used	0,4	NS	D	D

The expert is proposed to use linguistic values to evaluate all possible S_{3j} strategies. The choice of the linguistic term with its semantics is a very important issue. According to (Zadeh, 1999) fuzzy numbers support the semantics of the linguistic terms. It establishes the linguistic expression domain, in which experts provide their linguistic assessment of alternatives according to their knowledge.

In this section, we shall use labels represented by triangular fuzzy numbers. A triangular fuzzy number, denoted by M = <m, α, β>, has the membership function:

$$\mu_M\left(x\right)=\begin{cases} 0,\ \text{for } x\le m\le m - \alpha \\ 1-\dfrac{m - x}{\alpha},\text{for } m - \alpha < x < m \\ 1,\text{for } x = m \\ 0,\ \text{for } x \ge m+\beta. \end{cases} \qquad (12)$$

The point m, with membership grade 1, is called the mean value and α, β are the left hand and right hand spread of M respectively.

For example, we assign the following semantics to the set of three terms (graphically, see Figure 37):

NS = (0, 0,25, 0,5), S = (0,25, 0,5, 0,75), D = (0.5, 0,75, 1).

The aggregation stage: During this stage all linguistic values provided by experts are aggregated to obtain a collective assessment for the alternatives. It is provided by calculation of the fuzzy diversity score D_{ij} as an arithmetic mean:

$$\mathrm{D_{ij}} = (\frac{1}{t}\sum\nolimits_{i=1}^{t} \mathrm{w_k} \times \mathrm{m_{ij}^t}, \frac{1}{t}\sum\nolimits_{i=1}^{t} \mathrm{w_k} \times \alpha_{ij}^{t}, \frac{1}{t}\sum\nolimits_{i=1}^{t} \mathrm{w_k} \times \beta_{ij}^{t}) \tag{13}$$

Where w_k - weight of k diversity criterion; $< m_{ij}^t, \alpha_{ij}^t, \beta_{ij}^t >$ - a triangular fuzzy number that represents one of linguistic values {S, NS, D} assigned by *t*th expert for S_{ij} diversity strategy.

D_{ij} represents a distance between two objects: primary and secondary RTS. The more distance D_{ij}, which corresponds certain diversity strategy S_{ij}, the more diverse both RTSs. In this case, the primary RTS with its diversity attributes is considered as centre of cluster.

However, the final result is a fuzzy set, which does not correspond to any label in the original term set. In this case, "linguistic approximation" is needed (Zadeh, 1999). The process of linguistic approximation consists of finding a label, whose meaning is the same or the closest (according to some metric) to the meaning of an unlabeled membership function generated by some computational model.

It is worth to note that results, obtained by the fuzzy arithmetic, are fuzzy sets that usually do not match any linguistic term in the initial term set, so a linguistic approximation process is needed to express the result in the original expression domain.

Using the best-fit method (Dubois, et al., 1980), the obtained fuzzy diversity score D_{ij} for each strategies S_{ij} can be mapped back to one (or all) of the defined linguistic terms (SAME, NEARLY SAME, DIFFERENT). The method uses the distance between the fuzzy diversity score, represented by the fuzzy triangular number for each strategy S_{ij}, and each of the initial linguistic terms to represent the degree to which *obtained score,* is confirmed to each of them. For instance, the distance between the obtained fuzzy diversity score D_{ij} and the expression same, nearly same, different is defined as follows:

$$\mathrm{d_{ij}^{(r)}}\left(\mathrm{D_{ij}},\ \mathrm{SAME}\right) = \left[\sum\nolimits_{j=1}^{3}\left(\mu_{\mathrm{Dij}}^{j} - \mu_{\mathrm{same}}^{j}\right)^{2}\right]^{\frac{1}{2}};$$

$$\mathrm{d_{ij}^{(r)}}\left(\mathrm{D_{ij}},\ \mathrm{NEARLY\ SAME}\right) = \left[\sum_{j=1}^{3}\left(\mu_{\mathrm{Dij}}^{j} - \mu_{\mathrm{NS}}^{j}\right)^{2}\right]^{\frac{1}{2}};$$

$$\mathrm{d_{ij}^{(r)}}\left(\mathrm{D_{ij}},\mathrm{DIFFERENT}\right) = \left[\sum\nolimits_{j=1}^{3}\left(\mu_{\mathrm{Dij}}^{j} - \mu_{\mathrm{different}}^{j}\right)^{2}\right]^{\frac{1}{2}}; \tag{14}$$

Hence, each S_{ij} diversity strategy is characterized by 3-tuple $< d_{ij}^{(1)}, d_{ij}^{(2)}, d_{ij}^{(3)} >$, where, $d_{ij}^{(r)}$ a distance between the obtained fuzzy diversity score and the corresponding linguistic term (SAME, NEARLY SAME, DIFFERENT).

It should be noted that each, $d_{ij}^{(r)}$ (j=1,…J, where *j* – a number of possible alternatives classified as a type of S_i strategy) is an unsealed distance. The closer D_{ij}, is to the *r*th expression, the smaller $d_{ij}^{(r)}$ is. More specifically, $d_{ij}^{(r)}$ is equal to zero if D_{ij}, is just the same as the *r*th expression in terms of the membership functions. In such a case, D_{ij} should not be evaluated to other expressions at all due to the exclusiveness of these expressions. To embody such features, new indices need to be defined based on $d_{ij}^{(r)}$ (r = 1, 2, 3).

Suppose $d_{ij}^{(3)}$ is the smallest among the obtained distances for D_{ij}, and let α_{i1}, α_{i2}, α_{i3} represent the reciprocals of the relative distances between the identified fuzzy diversity score D_{ij}, and each of the defined linguistic terms with reference to $d_{ij}^{(3)}$ (smallest distance). Then, $a_{ij}^{(r)}$ (r= 1, 2, 3) can be defined as follow:

$$\alpha_{ij}^{(r)} = \frac{1}{\frac{d_{ij}^{(r)}}{d_{ij}^{(3)}}}, r = 1,2,3. \tag{15}$$

If $d_{ij}^{(3)} = 0$ it follows that $a_{ij}^{(3)}$ is equal to 1 and the others are equal to 0. Then, $a_{ij}^{(r)}$ (r = 1, 2, 3) can be normalized by:

$$\beta_{ij}^{(r)} = \frac{\alpha_{ij}^{(r)}}{\sum_{r=1}^{3} \alpha_{ij}^{(r)}}, \ r = 1,2,3. \tag{16}$$

Each $\beta_{ij}^{(r)}$ represents the extent, to which D_{ij} belongs to the *r*th defined linguistic terms. It can be noted that if D_{ij}, completely belongs to the *r*th expression, then it is equal to 1, and the others are equal to 0. The sum of values of these indices for D_{ij}, is equal to 1. Thus, $\beta_{ij}^{(r)}$ could be viewed as a degree of confidence that obtained fuzzy scores for all diversity strategies S_{ij} belong to the *r*th defined linguistic terms.

Results obtained for all diversity strategies are represented in the Table 12.

Table 12. Results obtained for all diversity strategies

Diversity Strategies	Degree to which D_{ij} belongs to the Initial Terms		
	Same	Nearly Same	Different
S_{31}	0,12	0,39	0, 49
S_{32}	0, 36	0,28	0,38
S_{33}	0,33	0, 63	0, 04

The exploitation stage: During this stage all diversity strategies are ranked by using the collective linguistic assessment obtained in the previous stage, taking into account the cost of each diversity strategies C_{ij}. The rational diverse strategy could be found with the following criterion:

$$S_{ij}^{*} = \operatorname{argmax} \frac{\beta_{ij}^{(r)}}{c_{ij}^{*}} \tag{17}$$

where $\beta_{ij}^{(r)}$ represents the extent to which D_{ij} belongs to the *r*th defined linguistic terms; C_{ij}^{*} - cost of S_{ij} reduced to $\sum C_{ij}, ij$ – number of diversity strategy.

According to the cost-effective approach suggested in the section, the strategy S_{31} (the primary RTS is FLASH – based RTS (A3PE1500, ProASIC 3/E family, Actel) and the secondary RTS – FPGA SRAM – based RTS (EP1SGX40G, Cyclone IV GX family, Altera)) might be recommended as a secondary one.

The selection of the rational diverse alternative is based on processing of the expert's judgment, represented as linguistic values on each of the diversity criterion. Two additional diversity strategies are represented. Each diversity strategy is characterized by the fuzzy diversity score of similarity (difference) between a proposed alternative for the secondary RTS and fixed primary RTS. The cost of strategy realization is also taken into consideration. The rational diversity strategy is taken with the suggested criterion. This approach might be useful during the initial stage of modernization of RTS, when a decision–maker is suggested to complete the initial set of alternatives for the primary RTS, which has been already determined. This stage is characterized by a high degree of uncertainty. When the initial set of diversity strategies is evaluated, it might be recommended to amend the given decision by application of metric-oriented methods.

Solution and Recommendations

Described models of multi-version systems are a base for the development of different architecture variants. The proposed techniques of diversity level and multi-version systems safety assessment are founded on two interconnected approaches. First of them is the metric-based technique allowing to assess a diversity level and to compare multi-version systems on application of different kinds and different volume of diversity. Second one is based on the probabilistic models, which include β calculated using metric analysis.

Development and implementation of multi-version FPGA-based systems is a new stage of the evolution in area of improving safety of NPP I&Cs. In this chapter we discussed basic concepts of diversity as a key approach to decreasing a probability of a common cause failure of safety-critical I&Cs and the taxonomic scheme of multi-version computing as a part of dependable, safe and secure computing.

Known version redundancy classification schemes were generalized in three-space matrix ("cube of diversity") taking into account features of FPGA technology. This unique technology allows to simplify NPP I&C development and verification, realize multi-reconfiguration (dynamical function- and dependability-oriented architecting, multi-parametrical space-structural adaptation, etc.), to propose decisions with different product-process version redundancy.

Key challenges related to diversity-oriented and FPGA-based systems are the following: existing standards are not enough detailed to make all necessary decisions concerning diversity (all the more FPGA-based decisions); multi-version I&Cs are still unique, failures occurred rarely and information about failures is not enough representative; methods of diversity assessment and kind selection, as a rule, are based on expert approach.

FPGA technology allows developing multi-version systems with different product-process version redundancy, diversity scalable multi-tolerant decisions for safety-critical NPP I&Cs.

FUTURE RESEARCH DIRECTIONS

Future R&D steps may be the following:

- Development of the detailed standards and guides to assess and choice types and capacity of diversity according to requirements and criteria of safety and cost.
- Research of different diversity types application to decrease risks of CCF taking into consideration dependencies of these types.
- Development of Safety Case-oriented techniques and tools for diversity assessment.
- Research and development of diversity application techniques for cyber security improvement taking into account features of MP and FPGA technologies.
- Analysis of diversity approach for System-on-Programmable Chip (Network-on-Chip, System-in-Package) and research of SoPC-based multi-version I&C systems.

CONCLUSION

Application of the diversity allows a decrease in the probability of CCFs. A new graphical model is presented in this chapter for different variants of diversity and can be used during the development of safety-critical systems and selection of optimal algorithms for diversity types based on a criterion of safety-reliability-cost. The model addresses diversity types at different levels: complex electronic components (FPGA, etc.), printed circuit boards, manufacturers, specification languages, design and program languages, etc. It takes into consideration the dependencies among diversity types. The graphical model is developed using the subgraph splitting algorithm, which has been previously used for software test generation.

Key challenges related to MP- and FPGA-based multi-version I&C systems concern uniqueness of ones, specific risks of CCFs (including CCFs for different versions of MVS) existing standards (are not enough detailed), approved diversity-oriented assessment techniques. One of the main challenges related to diversity approach is a fact that multi-version I&C systems are still unique, failures occurred very rarely and information about failures is not enough representative.

Analysis of NUREG 7007-and CLB (GMB)-based assessment techniques allows determining advantages/disadvantages of these techniques, possibilities of their joint applications and tool support. It the chapter three-stages CLD-MAD-RMD-technique for the assessment of multi-version NPP I&C systems is proposed. This technique has got an approbation in the analysis of multi-channel FPGA-based I&C Systems based on Radiy Platform and allows to decide the issue of assessment in conditions of lack of the statistical data about CCF.

REFERENCES

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, *1*, 11–33. doi:10.1109/TDSC.2004.2

Bakhmach, E., Kharchenko, V., Siora, A., Sklyar, V., & Tokarev, V. (2009). Advanced I&C Systems for NPPS Based on FPGA Technology: European Experience. Paper presented at the meeting of the *17th International Conference on Nuclear Engineering, Belgium.*

Bobrek, M., Bouldin, D., Holkomb, D., et al. (2009). Review guidelines for FPGAs in nuclear power plants safety systems. NUREG/CR-7006 ORNL/TM-2009/020.

Bukowsky, J., & Goble, W. (1994). An Extended Beta Model to Quantize the Effects of Common Cause Stressors. Paper presented at the meeting of the *ISAFECOMP, London.*

Dubois, D., & Prade, H. (1980). *Fuzzy Sets and Systems: Theory and Application*. New York: Academic.

Duzhyi, V., Kharchenko, V., Starov, O., & Rusin, D. (2010). Research Sports Programming Services as Multi-version Projects. *Radioelectronic and Computer Systems*, *47*, 29–35.

Gorbenko, A., Kharchenko, V., & Romanovsky, A. (2009). Using Inherent Service Redundancy and Diversity to Ensure Web Services Dependability In Methods, Models and Tools for Fault Tolerance, M. Butler, C. Jones, A. Romanovsky, E. Troubitsyna (Eds.), pp. 324-341, LNCS 5454, Springer.

Jonson, G. (2010). The INSAG Defense in Depth Concept and D-in-D&D in I&C. Paper presented at the meeting of the *7th ANS Topical Meeting on NPIC-HMIT, Las Vegas, USA*.

Kharchenko, V. (1999). Multi-version Systems: Models, Reliability, Design Technologies. *The 10th ESREL Conference: Vol.1, pp. 73-77.* Munich, Germany.

Kharchenko, V. Siora O., Sklyar V. (2011). Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring, Nuclear Power - Control, Reliability and Human Factors, Dr. Pavel Tsvetkov (Ed.), InTech, from: http://www.intechopen.com/books/nuclear-power-control-reliability-and-human-factors/multi-version-fpga- based-nuclear-power-plant-i-c-systems-evolution-of-safety-ensuring.

Kharchenko, V., Duzhyi, V., Sklyar, V., & Volkoviy, A. (2012). Safety Assessment of Multi-version FPGA-based NPP I&C Systems: Theoretical and Practical Issues. Paper presented at the meeting of the *5th International Workshop on the Applications of FPGA in Nuclear Power Plants, Beijing.*

Kharchenko, V., Siora, A., & Bakhmach, E. (2008). Diversity-scalable decisions for FPGA-based safety-critical I&C systems: from Theory to Implementation. Paper presented at the meeting of the *6th Conference NPIC&HMIT, Knoxville, USA*.

Kharchenko, V., Siora, A., Sklyar, V., & Volkoviy, A. (2012). Defence-in-Depth and Diversity Analysis of FPGA-based NPP I&C Systems: Conception, Technique and Tool. Paper presented at the meeting of the *ICONE20, Anaheim, USA*.

Kharchenko, V., Siora, A., Sklyar, V., Volkoviy, V., & Bezsaliy, V. (2010). Multi-Diversity Versus Common Cause Failures: FPGA-Based Multi-Version NPP I&C Systems. Paper presented at the meeting of the *7th Conference NPIC&HMIT, Las-Vegas, USA*.

Kharchenko, V., & Sklyar, V. (Eds.). (2008). *FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment, RPC Radiy, National Aerospace University "KhAI"*. State Scientific and Technical Center for Nuclear and Radiation Safety.

Kharchenko, V., Sklyar, V., Siora, A., & Tokarev, V. (2008). Scalable Diversity-oriented Decisions and Technologies for Dependable SoPC-based Safety-Critical Computer Systems and Infrastructures. Paper presented at the meeting of the *IEEE International Conference on Dependability of Computer Systems, Szklarska Poreba, Poland.*

Kharchenko, V., Sklyar, V., & Volkoviy, A. (2007). Multi-Version Information Technologies and Development of Dependable Systems out of Undependable Components. Paper presented at the meeting of the *International Conference on Dependability of Computer Systems,Szklarsla Poreba, Poland.*

Kharchenko, V., Yastrebenetsky, M., & Sklyar, V. (2004). Diversity Assessment of Nuclear Power Plants Instrumentation and Control Systems, *The 7th International Conference on PSAM and ESREL Conference, Volume 3, pp.1351-1356.* Berlin, Germany.

Mendel, J. M. (2002). An architecture of making judgment using computing with words. *International Journal of Applied Mathematics and Computer Science*, *12*(3), 325–335.

Naser. (Ed.). (2009). Guidelines on the use of field programmable gate arrays (FPGAs) in nuclear power plant I&C systems. Palo Alto, CA: EPRI.

NUREG/CR-6003. (1994). *Method for performing diversity and defense-in-depth analyses of reactor protection systems*. Washington, DC: United States Nuclear Regulatory Commission.

NUREG/CR-7007. (2009). *Diversity strategies for NPP I&Cs*. Washington, DC: United States Nuclear Regulatory Commission.

Prokhorova, Y., Kharchenko, V., Ostroumov, B., Ostroumov, S., & Sidorenko, N. (2008). Dependable SoPC-Based On-board Ice Protection System: from Research Project to Implementation. Paper presented at the meeting of the *IEEE International Conference on Dependability of Computer Systems, Szklarska Poreba, Poland.*

Pullum, L. (2001). *Software fault tolerance techniques and implementation*. Artech House Computing Library.

Siora, A., Krasnobaev, V., & Kharchenko, V. (2009). *Fault-Tolerance Systems with Version-Information Redundancy*. Ukraine: Ministry of Education and Science of Ukraine, National Aerospace University KhAI.

Siora, A., Sklyar, V., Rozen, Yu., Vinogradskaya, S., & Yastrebenetsky, M. (2009). Licensing Principles of FPGA-Based NPP I&C Systems. Paper presented at the meeting of the *17th International Conference on Nuclear Engineering, Brussels, Belgium.*

Sommerville, J. (2011). *Software engineering* (9th ed.). Reading, MA: Addison-Wesley.

Tarasyuk, O., Gorbenko, A., Kharchenko, V., Ruban, V., & Zasukha, S. (2011). Safety of Rocket-Space Engineering and Reliability of Computer Systems: 2000-2009 Years. *Radio-Electronic and Computer Systems*, *11*, 23–45.

Vilkomir, S. (2009). Statistical testing for NPP I&C system reliability evaluation. Paper presented at the meeting of the *6th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, Knoxville, USA*.

Vilkomir, S., Swain, T., & Poore, J. (2009). Software Input Space Modeling with Constraints among Parameters. Paper presented at the meeting of the *33rd Annual IEEE International Computer Software and Applications Conference COMPSAC, Seattle.*

Zadeh, L. (2009). From computing with numbers to computing with words-from manipulation of measurements to manipulation of perceptions. *IEEE Trans.Circ.Syst, Fund. TheoryApplic.*, *4*(1), 105–119.

Zadeh, L., & Kacprzyk, J. (1999). Computing with Words in Information/Intelligent Systems – Part 1:Foundation; Part 2: Applications. *Heidelberg, Germany*. *Physica-Verlag*, *1*, 187–201.

ADDITIONAL READING

Kharchenko, V. (1996). Theoretical foundations of fault-tolerant systems with version redundsncy. Kharkiv Military University, 1996, 506 p.

Littlewood, B., & Popov, P. et al. (2000). Littlewood B. Modelling the effects of combining diverse software fault removal techniques. *IEEE Transactions on Software Engineering*, *SE-26*(12), 1157–1167. doi:10.1109/32.888629

Littlewood, B., & Strigini, L. (2000). A discussion of practices for enhancing diversity in software designs. Littlewood B. *DISPO Project Technical Report LS-DI-TR-04. – Centre for Software Reliability, London, UK, 2000, 55 p.*

Littlewood, B., & Strigini, L. (2004). Redundancy and diversity in security. *Littlewood B. Proc. 9th European Symposium on Research in Computer Security (ESORICS'2004), France, 2004, p. 117–126.*

Medoff, M., & Faller, R. (2010). *Functional Safety – An IEC 61508 SIL 3Compatible Development Process. Exida.com L.L.C.* PA, USA: Sellersville.

Popov, P., & Strigini, L. (1998). Conceptual models for the reliability of diverse systems – new results. *Proc. 28th International Symposium on Fault-Tolerant Computing (FTCS-28). – Munich, Germany, 1998, p.80-89.*

Popov, P., Strigini, L., & Romanovsky, A. (2001). Diversity for Off-The-Shelf Components // *Proc. The International Conference on Dependable Systems and Networks – Goteborg, Sweden, 2001, p. 61-67.*

Smith, D., & Simpson, K. (2004). *Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards*. Oxford, UK: Elsevier Butterworth-Heinemann.

KEY TERMS AND DEFINITIONS

Diversity or Multiversity (MV): A principle providing use of several non-trivial versions. This principle means performance of the same function by two and more options and processing of data received in such ways for checking, choice or formations of final or intermediate results and decision-making on their further use.

Multi-Diversion System: MVS, in which two or more VR types are applied.

Multi-Version Project: (MVP): A project, in which the multi-version technology is applied (version redundancy of processes is used) leading to creation of one- or multi-version system (realization of version redundancy of products).

Multi-Version System (MVS): A system, in which a few versions-products are used; one-version systems may be redundant but consist of a few trivial versions.

Multi-Version Technology: (MVT): Set of the interconnected rules and design actions, in which in accordance with MV strategy a few versions-processes leading to development of two or more intermediate or end-products are used.

Strategy of Diversity: A collection of general criteria and rules defining principles of formation and selection of version redundancy types and a volume or/and choice of MVTs.

Version: An option of the different realization of an identical task by use software, hardware or FPGA-based products and life cycle processes.

Version Redundancy: A type of product and process redundancy allowing to create different (non-trivial) versions.

Chapter 7
Security of Safety Important I&C Systems

Vyacheslav Kharchenko
National Aerospace University named after N.E. Zhukovsky KhAI, Ukraine & Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Andriy Kovalenko
Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Anton Andrashov
Research and Production Corporation Radiy, Ukraine

ABSTRACT

One of the most challenging modern problems—security assessment and assurance for safety important I&C systems—is discussed. Interrelations and hierarchical structure of I&C systems attributes, including safety and security, are considered. Review of existing regulatory documents that covers various development and operation aspects of safety important I&C systems is presented. Such a review also addresses issues related to requirements for safety important I&C systems, including security requirements, depending on their underlying technology, as well as reveals the impact of the main features, including used technologies and development approaches. Main challenging problems and requirements in the area of security assurance for complex safety important I&C systems are outlined. A possible way to analyze the security vulnerabilities of safety important I&C system is considered; it is based on process-product approach, and it requires performance of assessments for products (components of I&C system at different life cycle stages) and all the processes within the product life cycle. A possible approach to assessment and assurance of safety important I&C systems security is discussed. Such an approach takes into account possible vulnerabilities of Field Programmable Gate Arrays (FPGA) technology and appropriate points of their insertion into the life cycle. An analysis of existing techniques for assurance of safety important I&C systems security is performed.

DOI: 10.4018/978-1-4666-5133-3.ch007

INTRODUCTION

I&C systems are complex systems that consist of both hardware and software components, which continuously interact with each other in order to perform their intended functions. One of the development and operation problems of modern I&C systems for critical application is the reliable assessment and assurance of the two main system attributes, namely safety and security. The assessment of security, which also influences the safety of I&C systems and other controlled applications, is a very important, complicated, and challenging problem. During the assessment, it is necessary to take into account a set of various features and factors, their interrelations and interactions. Modern realities require improving I&C systems security, both in terms of requirements and their implementation. Moreover, assurance of security for critical I&C systems is a requirement of national and international regulatory documents, as well as actual practice in safety engineering (IEC 61508, 2010).

The FPGA technology is now being widely used worldwide in process industries and increasingly in I&C systems for various safety and security critical domains, such as Nuclear Power Plants (NPPs), on-board computer-based systems, electronic medical systems, etc. (NUREG/CR-7006, 2010). The application of FPGA technology allows developers to implement the required functions in a convenient and reliable way.

There are several challenging problems in the area of security assurance for complex safety important I&C systems, including the following: consideration of all possible vulnerabilities that can appear in the final product due to process discrepancies, which were presented at earlier stages of the product life cycle, prioritization of such vulnerabilities according to their criticality and severity, determination of both sufficient and cost-effective countermeasures either to eliminate the identified (or potential) vulnerabilities or to make the vulnerabilities difficult to exploit by an adversary. In our opinion, the accurate evaluation of the actual level of the vulnerabilities' criticality and severity (and security of the system in whole) is one of the main challenges. Inaccurate estimation can cause additional efforts, costs and may present undesirable level of risk. In the framework of this chapter, I&C safety is considered as an attribute of high importance. Security is an attribute, which affects safety (Kharchenko, V. et al., 2011).

BACKGROUND

In a modern world, there are many various regulations, which, in general case, cover the most important areas widely used by the mankind. It is possible to distinguish those related (in some way) to safety important I&C systems, grouped into several sets to cover general issues of critical I&C systems at various lifecycle stages (including their development, operation and maintenance), security, as well as covering various technology-related aspects.

But a problem of creating of regulatory base covering simultaneously all the aspects required to develop, use and maintain reliable and secure safety important I&C systems is still challenging. Such regulatory base should also address questions related to processes and products depending on intended use of safety important I&C system, assessment and assurance of certain I&C system attributes, etc.

STATE-OF-ART DOCUMENTS IN THE AREA OF CYBER SECURITY

This subsection provides analysis results for existing documents, both national and international, related to the security of safety important I&C systems.

Research and Engineering Issues

Here we provide short reviews of the most important publications in the area of safety important systems security.

Ravi S. et al. (Ravi, S. et al., 2004) describe security-related gaps, unique to commercial embedded system design only. Importance and uniqueness of the embedded security challenges, an enumeration of security requirements, concepts, and design challenges are presented. Though, the paper is limited to security processing requirements and architecture, illustrated with a popular secure sockets layer protocol, and processing workload example.

Grand J. (Grand, J., 2004) introduces the concepts of designing secure hardware in embedded systems. The major classes of attacks and the mindset of potential attackers are presented, as well as examples of previous hardware attacks are discussed. Typical product development cycle and recommends ways to incorporate security, risk assessment, and policies into the process are presented.

Huffmire T. et al. (Huffmire, T. et al., 2010) provides comprehensive practical approach to managing security in FPGA designs, including both theoretical and practical aspects. It also addresses the lifecycle and operational threats against FPGA systems, as well as holistic view of FPGA security, from formal top level specification to low level policy enforcement mechanisms, which integrates recent advances in the fields of computer security theory, languages, compilers and hardware.

Badrignans B. et al. (Badrignans, B. et al., 2011) present an analysis of current threats against embedded systems and especially FPGAs. The requirements according to the FIPS 140-2 standard are discussed in order to build a secure system. Authors also highlight current vulnerabilities of FPGAs at all the levels of the security pyramid. Also several hardware solutions are described in this book especially at the logical, architectural and system levels (except operating system and application levels) to provide a global solution.

Sadeghi A.-R. et al. (Sadeghi, A.-R. et al., 2011) discover various issues related to physically unclonable functions, practical aspects of hardware-based cryptography, as well as problems related to policy enforcement, security in contactless tokens and security architectures and applications in embedded devices.

Drimer S. (Drimer, S., 2009) underlines importance of authenticating configurations as an additional capability to FPGA, proposes a security protocol for remote reconfiguration of FPGA-based systems over insecure networks. Some problems related to reproducing and comparing FPGA implementation results are discussed, as well as payment systems as ubiquitous embedded devices are examined and evaluated in terms of security vulnerabilities, including a man-in-the-middle attack.

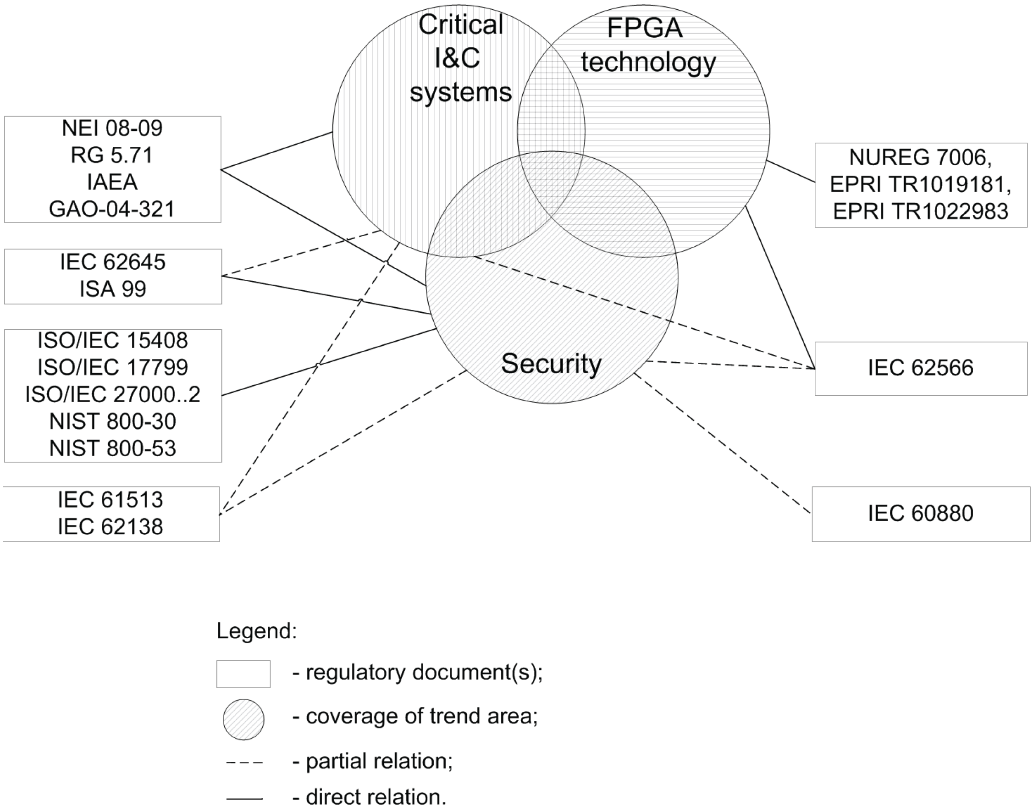
Regulation Issues

As for today, thorough the world there were developed a plenty of basic regulatory documents that cover various aspects in the areas of FPGA, critical I&C systems (including NPP I&C systems) and security. Regulatory documents in such particular areas try to form basement for developing secure (and reliable) I&C systems, which are capable to assure their intended functions (safety, security, etc.) through their life cycle. Regulatory documents pose general requirements, as well as they state the position and role of appropriate regulatory bodies.

As a result of conducted analysis partially based on (Kharchenko, V. et al., 2012,a), some of the existing standards and regulatory documents, both national and international, can be divided into the following main trend areas (see Figure 1):

- Regulatory documents related to critical I&C systems.

Figure 1. A classification of existing regulatory documents



- Regulatory documents related to FPGA technology.
- Regulatory documents related to security.

In the category related to critical I&C systems, one of the most important documents is a Committee Draft of IEC 62645 (IEC 62645, 2011). This document represents an approach to establishing requirements and providing guidance for the development and management of effective security programs for NPP I&C systems, implementation of life cycle for I&C system security and briefly describes main security controls. IEC 62645 is limited to security of NPP I&C systems and intended to be used when modernizing existing NPP and for designing new nuclear power plants, throughout the life cycle.

Modern standards such as the ISO/IEC 27000 series are not directly applicable to the cyber protection of critical I&C systems due to their specificities, including inherent regulatory and safety requirements. The focus of IEC 62645 is in issue of requirements for computer security programs and system development processes in order to prevent and/or minimize the impact of attacks against computer-based systems. This standard is based on ISO/IEC 27000 standards series and implies that any International Atomic Energy Agency (IAEA) and country specific guidance can expand area of the standard.

The ISA 99 series includes standards, recommended practices, technical reports, and related information that can define procedures for implementing electronic security measures and security practices, as well as approaches to assessment of their performance. The focus is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and to provide criteria for procuring and implementing secure control systems. Such documents assist in improving of manufacturing and control system electronic security, and can help identify vulnerabilities and address them to reduce the risk of compromising confidential information or causing system degradation or failure.

Series of ISA-99 standards include the following standards aimed to describe design and implementation process of security program for manufacturing and control systems:

- **ISA 99.00.01:** Scope, Concepts, Models and Terminology.
- **ISA 99.00.02:** Establishing a Manufacturing and Control Systems Security Program.
- **ISA 99.00.03:** Operating Manufacturing and Control Systems Security Program.
- **ISA 99.00.04:** Specific Security Requirements for Manufacturing and Control Systems.

Key moments, related to cyber security of manufacturing and control systems, and also aspects of design and implementation of security program are described.

In addition to the above standards the following technical reports are developed:

- **ISA TR 99.00.01:** Technologies for Protecting Manufacturing and Control Systems.
- **ISA TR 99.00.02:** Integrating Electronic Security into the Manufacturing and Control Systems Environment.

Technical reports contain:

- Recommendations for selection of technologies and measures of security assurance of assets and also the description of such technologies (including: authentication and authorization; filtering, access lock and control; audits, monitoring and detection; computer software; physical security measures).
- Guideline on design of electronic security program and also a recommended structure and content of security plan.

There are no existing regulatory documents that are specific about FPGA design practices. First referenced document in a category related to FPGA technology is NUREG/CR 7006, which was prepared by US Nuclear Regulatory Commission (NRC), and represents an attempt to cover existing gap.

This document is a comprehensive guidance for the NRC staff to confirm that FPGA-based safety systems are in conformance with the actual NRC regulations (moreover, some FPGA-specific review procedures and acceptance criteria during NRC-friendly licensing process can be based on this document). The document follows on the investigation of existing regulatory documents and standards related to design and review of safety-related FPGA systems.

NUREG/CR 7006 discovers various specific features of FPGA technology, including design practices, which are classified into three major groups – FPGA hardware design practices, FPGA design entry methods, and FPGA design methodologies. The document focuses on listing and describing FPGA design practices that are potentially unsafe as well as on suggesting, which ones are acceptable for safety-critical designs.

Additionally, the document outlines a design life cycle that could be used by the designers and the reviewers for FPGA-based safety systems. Also NUREG/CR 7006 presents results for survey of FPGA design guides and experience relevant to NPP application, as well as search results for technical standards related to FPGA design.

Next two documents (EPRI TR1019181, 2009 and EPRI TR1022983, 2011) were prepared by the Electric Power Research Institute (EPRI) in order to assist utilities in understanding, evaluating, and applying FPGA technology in NPP I&C systems and to address the use of FPGA technology in retrofits to operating NPPs and in new NPPs designs. These documents discuss advantages and limitations of FPGA technology on the basis of experience and lessons learned from previous applications, provide guidance on planning and conceptual design of modifications employing FPGA technology and on specifying and selecting FPGA-based systems; guidance on designing an FPGA application is also included, addressing the full life cycle of requirements, design, verification, and validation.

Category related to security is represented by IEC 62566. This document focuses on activities applied for developed Hardware Description Languages (HDL)-based integrated circuits (i.e. developed with HDL and related software tools) within an I&C system development project. In particular, it covers the following aspects: an approach to specify the requirements of, to design, to implement and to verify HDL-based integrated circuits, and to handle the corresponding aspects of system integration and validation; an approach to analyze and select the blank integrated circuits, micro-electronic technologies and Pre-Developed Blocks used to develop HDL-based integrated circuits; procedures for the modification and configuration control of HDL-based integrated circuits; and requirements for selection and use of software tools used to develop HDL-based integrated circuits.

In IEC 60880 standard (IEC 60880, 2006) only separate items are related to problems of security assurance. It is noted that main measures for software security assurance are applied at the systems level (for example, physical security measures).

Some requirements for minimization of software vulnerabilities related to supporting of protective measures, implemented at the system level, are presented, in particular:

- Requirements for software security analysis coverage.
- Requirements for accounting of the analysis results at different stages of software life cycle.
- Requirements related to users' access.
- Requirements related to security during software design process.

IEC 61513 standard (IEC 61513, 2011) contains security requirements at I&C system's architecture level and also at the level of their separate components. It is noted that software (code, parameters and data) is especially vulnerable during design and maintenance.

A general plan of safety assurance that determines procedural and technical measures used for protection of I&C architecture from both intentional and planned attacks is introduced. Also character is determined, and requirements for content of the systems security assurance plan are provided.

IEC 62138 standard (IEC 62138, 2004) supplements IEC 61513 with the following software requirements:

- Performing of threats and vulnerabilities analysis of I&C system software that takes into account security life cycle stages and determines requirements for protection, availability, privacy and integrity of data and functions (that can include: identification of security critical data and functions;

identification and authentication of personnel; control of access to security critical data and functions; data and function management; assignment of responsibility for security assurance and also traceability of executed activities).

- Performing of software design according to the security assurance plan or quality assurance plan, taking into account results of analysis of threats and vulnerabilities, and according to the general security assurance plan and system security assurance plan regulated by IEC 61513.
- With such a possibility, configuration and parameterization of software to avoid appearance of unnecessary vulnerabilities.
- Determination of resources for efficiency assessment for implemented solutions.

Document RG 5.71 (RG 5.71, 2010) is currently one of the most technically mature and complete of valid documents and describes the basis for realization of cyber security of facilities' assets related to nuclear power engineering (including a plan and a program of cyber security). In addition, the document contains safety requirements potentially applied to nuclear facilities.

According to the document, the problem of cyber security assurance for assets is reduced to protection against cyber attacks. The document determines requirements to cyber security program, for which designing, implementation and maintenance of cyber security plan are required (according to the given structure and guidelines), and also presents a short description of the appropriate stages and guidelines for their implementation.

Life cycle structure of cyber security process that includes the following stages is described: design of cyber security program, its implementation on facilities, continuous monitoring of the program, periodic program review, change management implementation and also retention of records and documentation.

For design, implementation and maintenance of cyber security program, the following series of activities is suggested:

1. Analysis of digital systems and networks of facilities.
2. Detection and assessment of critical assets from a safety point of view.
3. Implementation of security architecture according to the specified guidelines.
4. Analysis of potential risks of cyber security violation.
5. Implementation of maintenance activities for cyber security assurance program.

Multilayered architecture is suggested as the security architecture, and also a diagram of interaction of these layers and their description are provided.

Moreover, the document contains description of the following groups of safety assurance methods for each of security-critical assets, as well as approaches to their implementation:

- Technical methods for security assurance.
- Operational methods for security assurance.
- Executive methods for security assurance.

The document issued by IAEA (IAEA Nuclear Security Series No. 17, 2011) is IAEA manual for nuclear facilities, where application of computer security program is described. Importance of implementation of computer security aspects in a general security plan of facility is emphasized.

In contrast to RG 5.71 concepts of different safety types, including personnel, physical, cyber, computer security are introduced, and also a role of computer security is clearly outlined.

It is determined that all nuclear related facilities should have a standard, defining main tasks for computer security at facility and also a relevant plan. Importance of implementation of defense in depth strategy is emphasized. A concept and a diagram of security management life cycle and also key moments of its implementation are introduced. According to the document main life cycle stages are the following: review of (new) conception, requirements, design, implementation, operation, maintenance and continuous improvement.

In this document aspects of interaction between computer, physical and personnel security are also provided. In order to implement multilevel security approach, a structure of possible security levels is provided, and connection of system criticality levels with security assurance measures is shown. In addition, main security concepts and their interconnection are provided. In particular, concepts of countermeasures, vulnerabilities, risk, assets, threats, owner and attacker are defined.

It is also important that main approaches to risk assessment, risk management and detection and determination of vulnerability parameters are described. However, to estimate security indicators and support the decision making concerning set of the countermeasures it is needed to develop the techniques of security assessment, which could take into account features of software and FPGA-based systems.

The ISO/IEC 17799 standard (ISO/IEC 17799, 2005) contains guidelines concerning cyber security management and can be used during the development of security standards and the selection of practical activities for security management in organizations.

The standard determines:

- Organizational issues of security.
- Aspects of classification and management of organization's assets subjected to protection.
- Personnel related security issues.
- Elements of physical protection and protection against environmental impacts.
- Aspects of communication control and operating activities control.
- Approaches related to access control.
- Security requirements during system design and maintenance.

NEI 08-09 document (NEI 08-09, 2010) is the description of assets protection strategy consisted of security architecture and a set of methods of security assurance in nuclear facilities. This protection should be performed to comply with the requirements of 10 CFR 73.54.

The document contains a template of cyber security plan and description of applicable methods.

NIST 800-30 document (NIST 800-30, 2002) has a recommendatory nature and is a risk management technique that includes processes of risk assessment and risk reduction.

Definition of risk as a negative network impact that is caused by vulnerability and taken into account probability and a degree of such impact is provided.

Risk management includes processes of risk identification and assessment, as well as implementation of measures to reduce the risk to the acceptable level.

It is noted that implementation of risk management allows facility:

- To build better protection of own information systems, which storage, process or transfer data.
- To make reasonable solutions devoted to correction of costs related to information technologies.
- To support authorization/accreditation of information systems before commissioning via providing risk management documentation.

An order of risk assessment including the following steps is provided:

1. System description.
2. Identification of threats.
3. Identification of vulnerabilities.
4. Analysis of security assurance methods.
5. Determination of probabilities.
6. Impact analysis.
7. Risk determination.

8. Formulation of guidelines for application of security assurance methods.
9. Documenting of results.

It is noted that during implementation of recommended risk reduction measures technical, management and operational methods of security assurance methods and also their combination should be used to maximize their efficiency.

It is also noted that the success of risk management program implementation is caused by:

- Management policy.
- Participation of technical specialists.
- Competence of team, performing risk assessment (including interpretation of methodology of risk assessment for specific systems, risk identification, provision of profitable protective measures).
- Information awareness and collaboration of all participants involved into program.
- Constant assessment of risks of cyber security violation at the facility.

Cyber security requirements for critical infrastructures, including peculiarities and dynamics of threats, vulnerabilities, incidents and effects of potential attacks, are provided in GAO-04-321 document (GAO-04-321, 2004), and also a close relation of these concepts with information technologies is noted.

It is noted that the problem of cyber security assurance during power generation can be reduced to the problem of assurance of integrity, availability and privacy of relevant facility's assets.

Moreover, a list and description of general controls of security assurance for systems and networks (including access control, system integrity management, cryptography, audit and monitoring, as well as configuration management) are provided, and also main standards for all these controls are listed.

Some approaches for planning and implementation of cyber security assurance process are provided, including: determination of business requirements to security; risk analysis performance; introduction of security policy; implementation of measures of cyber security assurance (including personnel, processes and technologies devoted to decrease identified security risks); continuous security monitoring and management.

In the part devoted to risk management, a methodology of risk analysis is described. It is noted that risk assessment is a key aspect of cyber security. Risk assessment can be considered as a complex of sequentially implemented stages.

The first stage is the identification of facility's assets that should be protected and also possible effects of their loss.

At the next stage identification and determination of characteristics of threats for facilities are performed. During determination of threats criticality, main criteria are intentions and possibilities of an attacker.

The third stage includes identification and determination of characteristics of vulnerabilities, due to which threats can be made.

At the fourth stage risk assessment and determination of priorities for assets protection are performed. During risk assessment, a potential effect of asset loss or damage is considered. Levels of risks are determined according to the assessment of impact of asset loss or damage, asset threats and vulnerabilities.

Final stage consists in the identification of countermeasures for decreasing or elimination of risks and also in the performance of a comparative analysis of advantages and efficiency of such countermeasures with their disadvantages and cost.

NIST 800-53 document (NIST 800-53, 2009) has a recommendatory nature and is devoted to issues of selection and implementation of relevant methods of safety assurance of information systems. The detail description of implementation of each of the methods is provided.

The ISO/IEC 15408 standard (ISO/IEC 15408, 2009) introduces general principles and concepts of security assessment for information technologies and determines a general technique of the assessment, being a basis for assessment of security features of information technologies. Furthermore, an interconnection of high level security concepts is provided, and also an interconnection of security assessment concepts is reflected.

Moreover, the standard introduces requirements for a structure and content of security functional components for security assessment. A catalogue of functional elements, meeting general requirements of security functionality for many products from information technology field, is provided.

Therefore, the standard is a set of criteria that allows performing security assessment of information technologies.

Nowadays the problem of cyber security assessment and assurance for safety important I&C systems, especially in a context of used technologies, is not comprehensively solved due to several objective reasons. One of such reasons is insufficiently structured regulatory documents, both local and international: there is no special branch standard that covers cyber security aspects of FPGA-based critical I&C systems. Moreover, there are no strict interdependencies between the above regulatory documents, their coverage is insufficient, and the problem of their "branch customization" is still challenging.

Therefore, it is possible to conclude that existing regulatory documents represent an evolving area of regulatory requirements, try to cover the intended areas without sufficient consideration of related ones, and should be more detailed in terms of appropriate approaches and their relationship with the technologies.

SAFETY AND SECURITY CONCEPTS FOR I&C SYSTEMS

Nowadays safety important systems are widely used by the world industry in various areas in forms of I&C systems for NPPs, on-board computer-based systems, electronic medical systems, etc. Moreover, FPGA technology is now being trend in safety important systems implementation that inevitably leads to new challenges in various aspects of such systems design, operation and maintenance requiring new approaches, techniques and appropriate requirements.

The objective of this subsection is to provide a review of practical problems concerning safety and cyber security in modern I&C systems, including those based on FPGA technology application. Such review also involves threats related to trojans in hardware and tools (in particular, in FPGA chips and appropriate design tools used in development of I&C systems for critical applications), which can affect the functionality of hardware, as well as review of possible countermeasures to such threats.

Safety and Security Aspects

One of the most important attributes of safety important systems is dependability. Dependability of a system is the ability to deliver required services (or perform functions) that can justifiably be trusted. Dependability is a complex attribute of a safety important system that can be represented by a set of primary attributes, including:

- **Reliability:** Continuity of correct (required) services.
- **Availability:** Readiness for correct services.
- **Survivability:** Ability to minimize loss of quality and to keep capacity of fulfilled functions under failures caused by internal and external reasons.
- **Safety:** Absence of catastrophic consequences for the user(s) and the environment.
- **Integrity:** Absence of improper system alternations.
- **Confidentiality:** Absence of unauthorized disclosure of information.

- **High Confidence:** Ability of correct estimation of services quality, i.e. definition of trust level to the service.
- **Maintainability:** Ability to undergo modifications and repairs.
- **Security:** The protection from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

In turn, safety attribute of a safety important system can have some particular (or secondary) attributes depending on exact system, environment and conditions that have influence on the primary attribute. Here, we distinguished the following attributes (see Figure 2): reliability, security and trustworthiness, and we denoted their two-way influence (Kharchenko, V. et al., 2012,b).

We should note that such particular attributes may be defined for each of primary attributes, thus, representing hierarchical structure of safety important system's generic attributes set. Moreover, those secondary and further attributes may turn to be common for different primary attributes due to their incomplete "orthogonality."

Metrics

Thus, we can state that a set of safety important system attributes can be represented in a form of i-level hierarchical model, and each of i levels contains ki attributes. As an example, Figure 3 represents an element of last two levels of a safety

Figure 2. Taxonomy of safety attribute

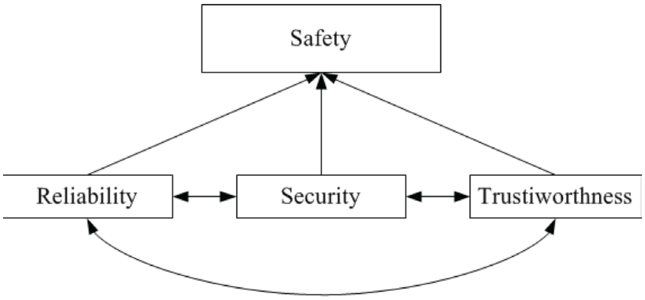
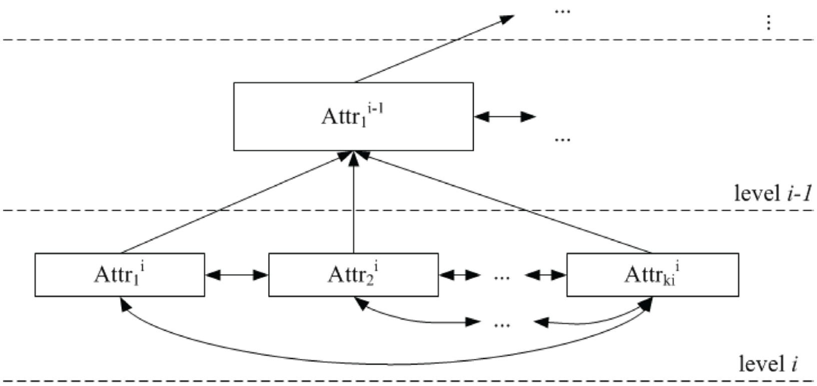


Figure 3. Levels of safety important system attributes hierarchy



important system attributes hierarchical model consisting of i levels.

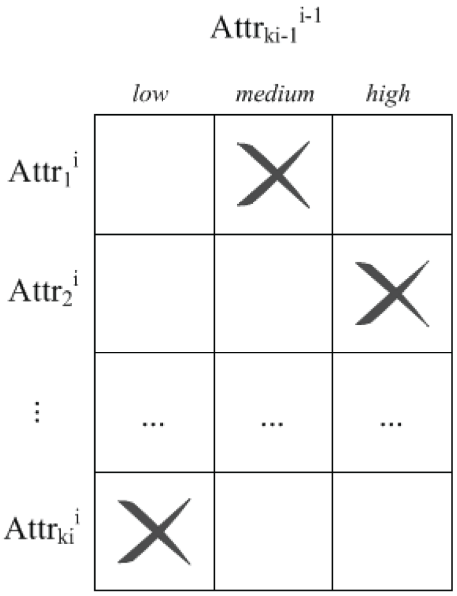
One of the possible ways to reveal criticality of two-way influence for safety important system's attributes is in creating of attributes influence matrix. Such a problem can be solved, in particular, in the following ways:

1. Create a set of *n* "local" influence matrixes for *i* hierarchical levels; each of the matrixes consists of k_i attributes (see Figure 4), and, therefore of k_i rows. Such number *n* can be calculated using the following equation:

$$n = \sum_{x=1}^{i-1} k_x \tag{1}$$

The number of rows in each matrix associated with the level *m*, where *m*=[1,*i*-1], is equal to a number of attributes (k_m) at the lower level *m*+1: for example, the local matrix for a single attribute of *i*-1 level consists of k_i rows.

Figure 4. Local influence matrix



$\mathrm{Attr}_{k_{i-1}}^{i-1}$

	low	medium	high
Attr_1^i		✕	
Attr_2^i			✕
⋮	...	...	...
Attr_{ki}^i	✕		

A set of such "local" influence matrixes represents the case of a metric mostly intended for independent assessment of the safety important system's attributes within the single level.

2. Create the single "global" influence matrix where each of all the *n* attributes (see Equation(1)) is reflected by a single row and appropriate column (see Figure 5).

"Global" influence matrix can be considered as another metric, which is suitable for assessment of the safety important system as a whole.

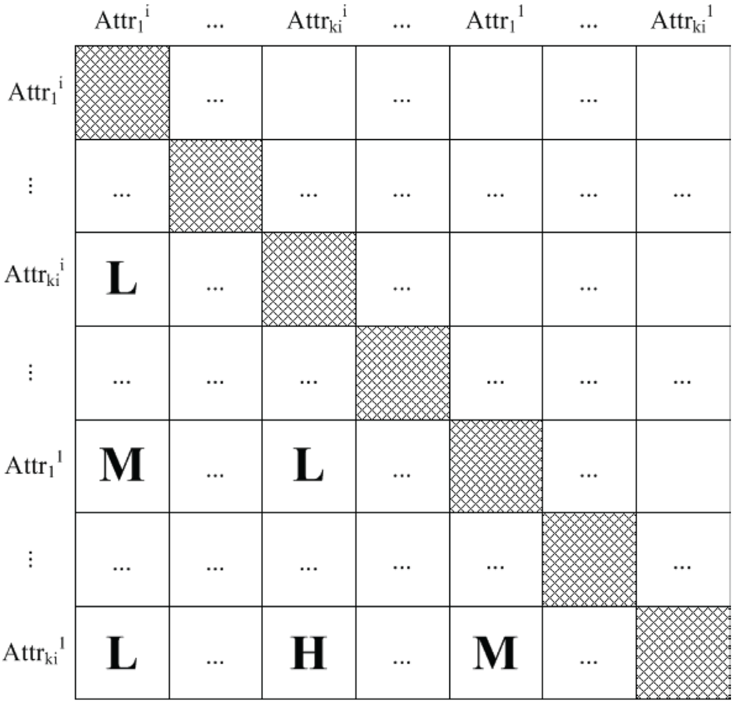
Thus, on the one hand, such metrics allow sharing SCS resources in order to assure the required level of security (a vertical related to different levels in Figure 3), on the other hand, they allow optimizing the use of the resources (within the same level, see Figure 3).

Cyber Security Threats and Vulnerabilities for FPGA-Based I&C Systems

At the present time, there is limited number of potentially probable modes of cyber attacks on FPGA technology, a list of which, along with their short description, harmonized with Badrignans B. et al., (Badrignans, B. et al., 2011), is given below.

1. **Black Box Attack:** An adversary inputs all possible combinations to FPGA chip and registers output states. Such an approach provides potential possibility of reverse engineering for FPGA electronic design, integrated into a chip. In practice this approach is extremely hard to implement for systems with complex logic.
2. **Read-Back Attack:** The attack is based on a potential possibility of reading FPGA chip configuration, usually, via JTAG interface used in most FPGAs for debugging. Recently, FPGA vendors have improved protection measures to access chip configuration (for

Figure 5. Global influence matrix



	$Attr_1^i$	...	$Attr_{ki}^i$	...	$Attr_1^1$	...	$Attr_{ki}^1$
$Attr_1^i$	▨	...		...		...	
⋮	...	▨	...	...	...	...	...
$Attr_{ki}^i$	**L**	...	▨	...		...	
⋮	...	...	...	▨	...	...	...
$Attr_1^l$	**M**	...	**L**	...	▨	...	
⋮	...	...	...	...	...	▨	...
$Attr_{ki}^l$	**L**	...	**H**	...	**M**	...	▨

example, it was implemented a security bit, which controls the readability of chip configuration) to resist such attacks.

3. **Cloning Attack:** In SRAM FPGA chips, a configuration file is stored in nonvolatile memory outside FPGA chip, allowing quite easily retrieve a bitstream while loading configuration in the FPGA and clone such FPGA electronic design of such chip afterwards. The only variant of protection against this threat is encrypting a bitstream during its transmission from a nonvolatile memory to the FPGA that has been already implemented in most modern FPGAs. Therefore, the strength of applied cipher is an open-ended question.
4. **Physical attack against SRAM-based FPGAs:** The objective of such an attack is to obtain information concerning physical structure of FPGA chip by studying specific areas in the chip. Such attacks are usually targeted on FPGA parts inaccessible through input-output channels. Instruments, based on focusing of ion beam, allowing FPGA structure checking, are used for the attack. It is rather difficult to implement such attack due to complexity of required equipment; besides that, some technologies (for example, Antifuse and Flash), which have their own restrictions, significantly complicate such mode of attacks.
5. **Side-Channel Attack:** Such an attack uses specifics of systems' physical implementation in order to obtain information concerning power consumption, execution time and electromagnetic fields, allowing an adversary to obtain power, time and/or electromagnetic signatures, which, in turn, can expose information about their underlying implementation. Hence, in order to implement side-channel attack, it is required to solve a task of obtaining such

signatures and a task of their processing for obtaining required results. Tasks of collecting and processing of such information are rather nontrivial, however, there are known complex techniques requiring only several measurements to attack a system.

Data Analysis: It is a logical continuation of read-back attack or side-channel attack, as data, obtained from these attacks, are considered as noise. The fact that an adversary has obtained such data does not guarantee a possibility of recovering original FPGA electronic design, but makes it probable.

Logically following stage after the read-back attack (or cloning attack) is Reverse Engineering. It allows, for example, discovering a data structure, used by the manufacturer, decrypting FPGA configuration. Reverse Engineering is not limited to discovering of FPGA configuration, but also can be achieved by observing bus activities during program execution in a softcore processor implemented in FPGA environment. Application of the reverse engineering technique is characterized by quite high percentage of its successful completion.

To retrieve data, an adversary can use approaches based either on Simple Power Analysis or Differential Power Analysis techniques. These approaches are based on device's energy consumption analysis, while performing cryptographic operations, depending on time and their identification with the known templates. So, a success of the attack directly depends on time and number of stored statistic data.

As of today, a number of factors that can cause FPGA vulnerabilities, which can be used in cyber attacks, should be identified. Such attacks can result in:

- Hardware modification, reading and/or distortion of confidential and/or critical information (for example, through side-channels).
- Addition of unintended functionality (for example, by development tools).
- Stealing of intellectual property.

So, it is possible to identify a number of factors that can cause vulnerabilities at different stages of FPGA chip life cycle (see Figure 6), including:

- A stage of FPGA chip design.
- A stage of its manufacturing and packaging.
- A stage of development of FPGA electronic design (which describes application logic) for implementation to FPGA chip.
- A stage of FPGA electronic design implementation.
- A stage of operation of FPGA-based device.

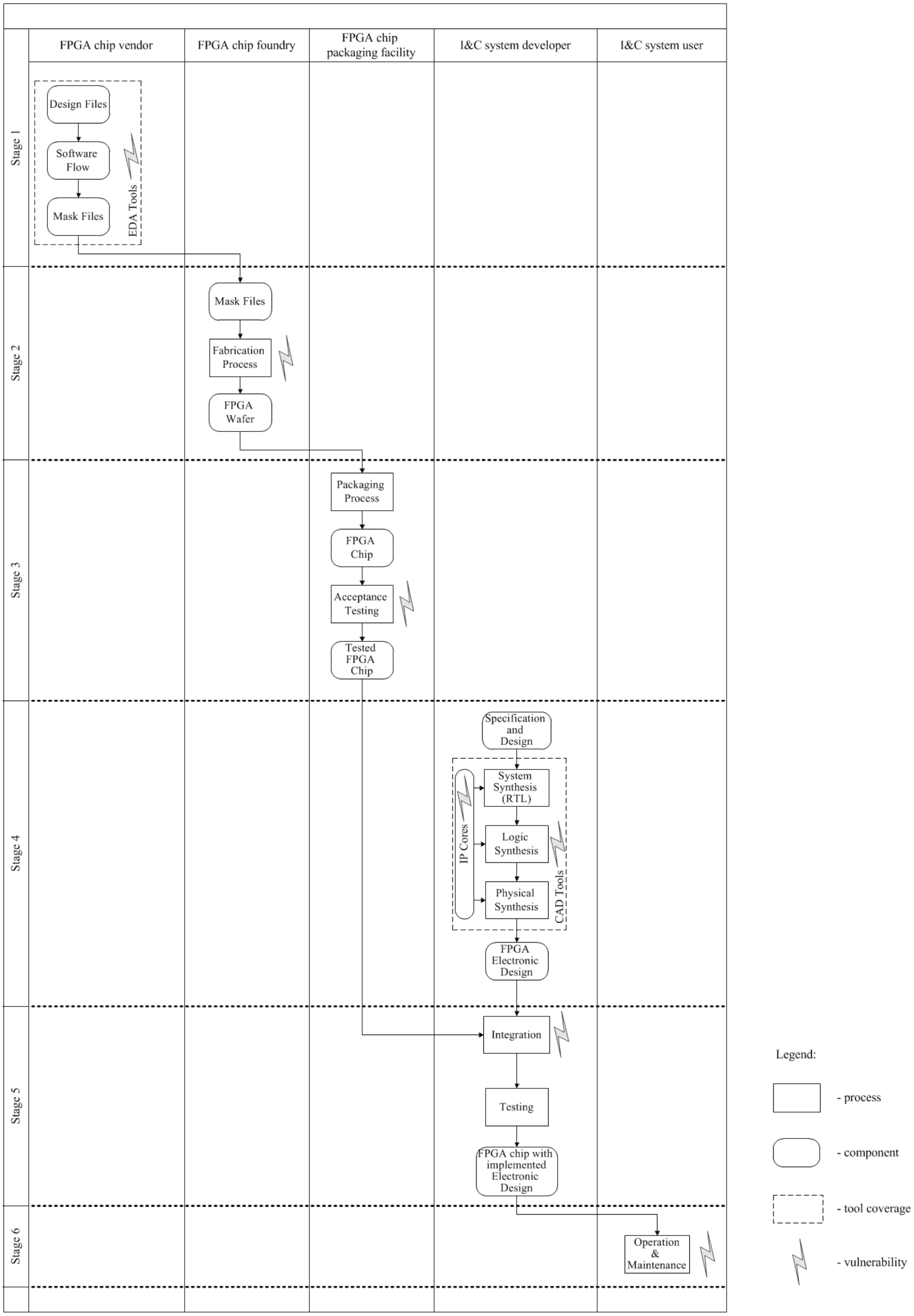
Such factors are the following:

- Use of malicious tools (EDA tools, CAD tools) during chip designing by a vendor and during FPGA electronic design development by an application designer for such chip;
- Use of compromised devices during integration of FPGA electronic design by an application designer;
- Use of IP-cores from third-party vendors in FPGA electronic design;
- The presence of adversaries (insiders) inside the development team.

To decrease number of FPGA potential vulnerabilities, FPGA chip vendors should solve the following tasks:

- To provide protection of own design and technology against reverse engineering, copying or modification.
- To provide the customers with design security means during development and operation FPGA-based devices.

Figure 6. Life cycle stages of FPGA chip and FPGA-based I&C systems with potential vulnerabilities



Most of the vendors of FPGA chips do not have their own manufacturing capacity: their task is in development of designs of FPGA chips (that includes application of tools for design automation) and placement of orders for their manufacturing among appropriate foundries. Such factories play important role in assurance of cyber security for future chips, as well as in prevention from probable vulnerabilities that can be caused by stealing or modification of FPGA design during chip manufacturing process.

On the other hand, vendors of FPGA chips facilitate distribution and safety integration of various IP-cores used by application designers to encourage FPGA chips market. IP-core is completed functional description intended for integration into electronic design, which is being developed. IP-cores are being often used by designers of FPGA-based applications to save resources and time. IP-cores can be either in a form of modules for hardware description languages (HDL) or in a form of compiled netlists. So, such IP-cores can introduce additional vulnerabilities into applications, which use them. Supply chain of chips is usually traceable and can be audited that, however, does not reduce its importance from FPGA cyber security assurance point of view.

Most of life cycle stages of FPGA chip are implemented using software tools. Such tools are usually used during design of printed circuit boards, integrated circuits, developing FPGA electronic designs and simulation. Hence, developers of tools for design automation play key role in FPGA cyber security assurance and, in turn, can cause vulnerabilities.

The objective of FPGA-based devices' cyber security assurance should be solved at different stages of hierarchy, as each of the stages has specific hardware or software vulnerabilities. Thus, the objective of cyber security assurance should be started from defining the boundaries of a system.

Hardware Trojans in Safety Important I&C Systems

One of the threats in I&C systems for critical applications is related to potential possibility of Hardware Trojans (HT) insertion into hardware. Hardware trojan is a harmful and intentionally hidden modification of electronic device (for example, chip or its internal programmable configuration). Such a modification can change functionality of a device, which contains digital integrated circuits and/or programmable components, or based on FPGA technology that will lead to its malfunction (for example, due to unpredictable failures and/or faults) and, thus, dent confidence in a system using this device.

Insertion of HT is possible at the stages of development and manufacturing of both FPGA chip and systems based on the chip.

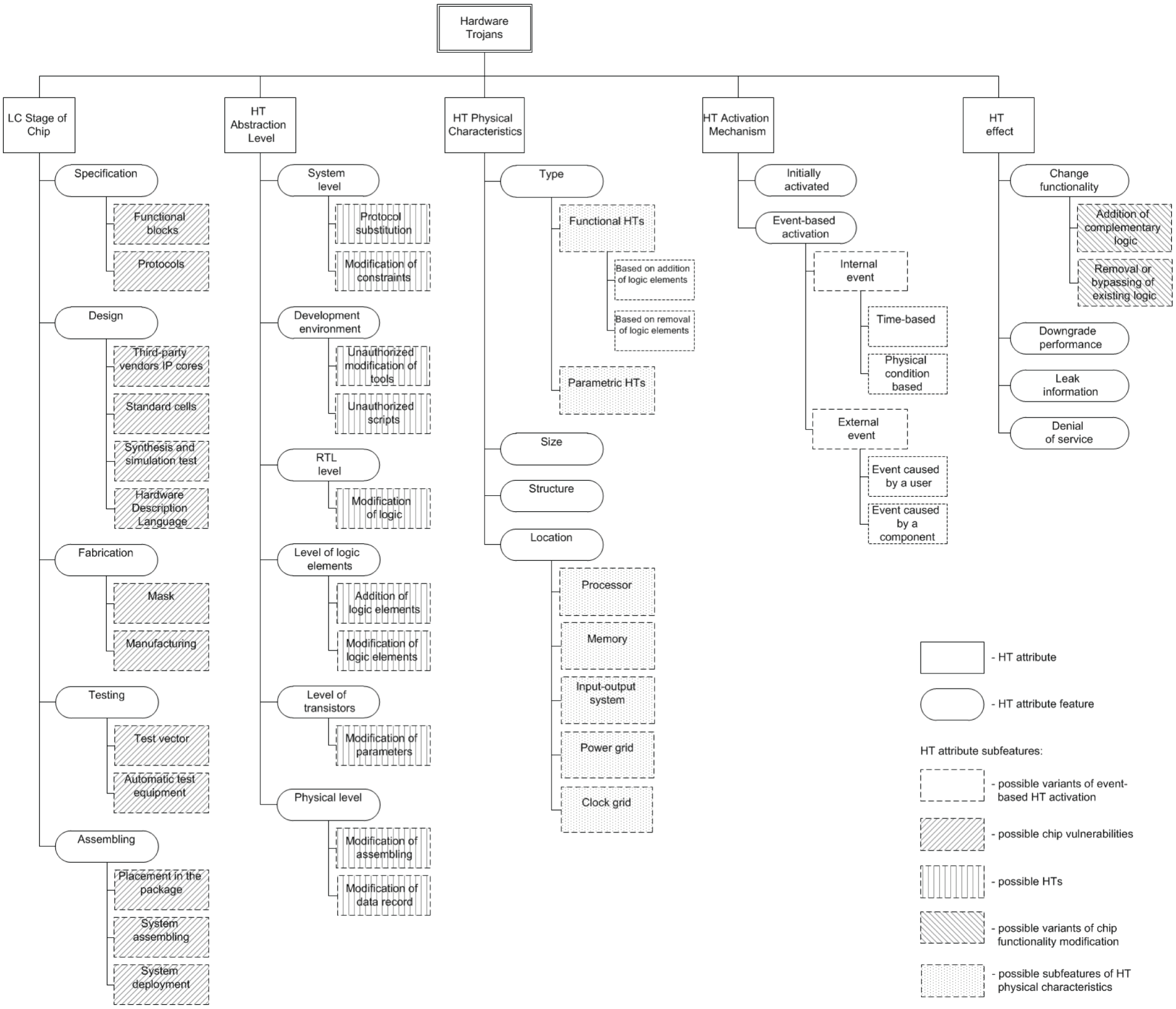
At the modern stage of development of system design technologies based on integrated circuits and/or programmable components, existence of a set of hardware trojans that have specific effect on device operation (for example, FPGA chip), in which they can be built in, is possible. Figure 7 depicts taxonomy, partly based on Karry R. et al., (Karry, R. et al., 2010), of HT based on the following attributes with specific features:

- A stage of chip life cycle (LC) at which HT is inserted.
- Abstraction level of which HT implementation.
- HT physical characteristics.
- HT activation mechanism.
- HT effect.

Each of the attributes is described below in details.

HT insertion is possible at the following stages of chip LC:

Figure 7. Taxonomy of hardware trojans



- **Specification:** At this stage designers determine main chip characteristics (for example, its target environment, expected functionality, physical size, power consumption and delays), therefore, a modification of such characteristics makes possible modification of functional specifications and design constraints (for example, timing requirements).
- **Design:** At this stage developers specify functional, logic, timing, and physical constraints so that a chip will conform to target technology, therefore, application of third-party vendor IP-cores and standard cells becomes possible during development process; so, HTs can be present in any of components that were used in chip development process;
- **Chip Fabrication:** At this stage a set of masks, using wafers, is created; even subtle mask modifications can seriously affect chip functionality;
- **Chip Testing:** This stage provides potential possibilities for HT detection inserted during previous LC stages of a chip;

- **Chip Packaging:** At this stage the tested chip is mounted into the chip package (it can also contain other hardware components); from vulnerability point of view, interfaces between all hardware components introduce potential vulnerabilities at this stage.

From abstraction level's point of view, HTs can be inserted into a chip at the following levels:

- **System Level:** Developers define hardware modules, interconnections and communication protocols, which can determine HT activation character.
- **Development Environment:** It can be characterized by application of tools for design synthesis, simulation, verification, and validation; such tools can be a source of HTs in the design and, moreover, contain software trojans for hiding inserted HTs.
- **RTL Level:** Is easily vulnerable by HTs, as at this level each functional module is described in terms of registers, signals and Boolean functions.
- **Level of Logic Elements:** A chip is represented as interconnection of logic elements that allows controlling all aspects of inserted HTs, including size and location.
- **Level of Transistors:** Logic gates are built from transistors, allowing managing different chip characteristics (for example, time characteristics and power consumption); addition or removal of individual transistors allows modifying chip functionality, and modification of transistor sizes lead to modification of chip parameters.
- **Physical Level:** This level describes all chip components, their physical size and location, that allows inserting HTs, for example, by modifying wire size, a distance between circuit elements or reassigning metal layers.

In general case, accordingly to Tehranipoor M. et al., (Tehranipoor, M. et al., 2010), HTs can be inserted into one or several system components. In the latter case, each of HTs can operate independently from other HTs, or together with other HTs inside the system to perform group attack on the system.

Depending on probable physical characteristics, HTs can be differed by:

- Type
- Size
- Structure
- Location

According to the type, HTs can be:

- Functional (implemented through addition or a removal of logic elements).
- Parametric (implemented through modification of a existing logic or connections).

According to location, HTs can directly affect the following components:

- Processor (HTs can modify an order of instructions execution).
- Memory, including its interfaces (HTs can modify values, stored in a memory, and also block reading/writing operations for certain memory areas).
- Input-output system (HTs can be located in peripherals of chip or device, as well as within printed circuit board, and, interacting with external components, control communications between a processor and external components of a system).
- Power circuitry (HTs can alter voltage and current supplied to chip or device, causing failures).
- Clock circuitry (HTs can change clock's frequency, supplied to different functional modules, causing faults inside the system, containing such modules).

Tehranipoor M. et al., (Tehranipoor, M. et al., 2010) distinguished the following activation mechanisms for HTs:

- **Initial Activation:** HT is activated (i.e. it is triggered without addition conditions or events) at the moment of chip fabrication.
- **Event-Based Activation:** HTs are being activated only by a specific internal or external event. Internal event is an event caused by a chip or device that contains HTs. Internal events can occur after predetermined time period or due to specific physical conditions (for example, chip temperature). Activation by an external event means that specific signal or combination of signals (for example, specified sequence in input data from the user) inputs a chip or device, which contains HTs, or data input through special port.

Effect of HT activation can vary from imperceptible disturbances in operation of device, which contains HT, to catastrophic failures of the system, which contains such device, and can be divided into the following groups:

- **Change device functionality (by addition of complementary logic, or removing/bypassing existing logic):** It mostly leads to subtle errors that are almost undetectable.
- Downgrade performance due to intentional change of device parameters by HT, and can be caused by functional characteristics or interface characteristics.
- Leak of information through overt or covert channels.
- **Denial of Service:** It prevents operation of function or resource, usually causing unexpected lack of bandwidth, computation or battery power; physical destroying, disabling or altering device's configuration is also possible.

All the approaches to HT detection can be divided into two categories: destructive and nondestructive.

Destructive approaches are based on demetallization process followed by scanning using an electronic microscope. Such approaches are extremely expensive and time-consuming (about several months for single chip), becoming ineffective when increasing of transistor density on the chip. Moreover, taking into account that only a small part of chips from a manufactured lot can contain HTs, such approaches can be considered as ineffective.

Nondestructive approaches, in turn, can be divided into two categories: invasive (based on modification of original FPGA electronic design in order to insert functions intended for HT detection) and non-invasive (do not require modification of original FPGA electronic design).

Invasive approaches to HTs detection in chips can be divided into two subcategories:

- Preventive (intended for prevention of insertion of HTs at the stages of chip development or fabrication).
- Assistive (intended for detection of inserted HTs into a chip).

A possibility of insertion of HT during chip design stage depends on availability of unused space (or possibility of obtaining such space via logic optimization of electronic design) within chip layout. Moreover, a complexity of insertion of HT into a chip significantly depends on a possibility of "masking" of original electronic design by vendors through expansion of reachable state space to make it difficult to reverse-engineer by adversaries the chip functionality and find the true rare events (so, inserted HTs by adversaries can have no effect on normal chip operation or become easily detectable).

For HTs detecting is possible to use approaches based on testing of chip logic or measuring parameters of chip side-channels, since an adversary uses rare internal states of the chip to construct HT. Also to detect HT, vendors can insert special "latches" into electronic design, responding to specified event, much more likely caused by HT in the chip.

Non-invasive approaches for HT detection consist in comparison of behavior of test FPGA chip and etalon chip (or etalon functional model). Hence, non-invasive approaches can be divided into the following subcategories:

- HT detection approaches used during chip operation (use real-time diagnostic system to detect HTs during normal operation of a chip).
- HT detection approaches used during testing (intended for detecting of HTs during chip testing, before its use).

All the approaches to HT detection, used during chip operation, require chip resources for their implementation (cause increase of power consumption), since they perform checks during normal chip operation, and, in a case of deviation, they trigger appropriate countermeasures. Such approaches are used as the last line of chip defense, providing absolute credibility of computed results, and can be based on any of the following principles:

- Use of novel bus architecture that can detect operating HTs inside the chip, activate protection against them, and also notify about such activity (such architecture requires about 800 logic elements for the chip, which contains 4 millions of logic elements, and cause minor delays).
- Use of scheme that implements (by hardware) HT detection functionality in several chips simultaneously and compares them in order to dynamically assess their trust-levels.
- Use of combined hardware-software approach that consists in using of simply verifiable hardware module external to the chip, allowing detecting DoS-attacks and privilege escalation attacks (attacks can be detected using periodic checks and cause decrease of mean performance level by several percent).

Approaches to HT detection, used during chip testing, can be based on logic checking or measurement of side-channel parameters (for example, power, delays, etc.). Advantage of such approaches is that their implementation does not require resources overhead for test chips. The only disadvantage consists in that there should be etalon ("golden") chip similar to the test chip, but without HTs inserted inside.

The only disadvantage of approaches to HTs detection that are based on logic testing, is the enormously large HTs space, which makes the generation of an exhaustive set of test vectors to detect all possible HTs computationally infeasible. Logic testing-based approaches can be based on the following principles:

- Use of a technique based on inserting randomization elements for probabilistic comparison of functionality of manufactured chip with its electronic design.
- Generation of statistical vector, which represents an optimal set of test vectors, allowing trigger specified (often rarely used) node in a circuit to its rare value multiple times.

Side-channel parameters analysis-based approaches for HT detection are based on the following assumption. Even if HT presence inside a chip does not cause visible deviations during testing, then HT presence could be detected by monitoring the effect on such physical parameter such as chip current transient, power consumption or path delay. At the present time, main difficulties for application of this approach are large process variation (due to modern chip nanometer technologies) and noises during parameters' measurement (that can lead to masking of disturbances, generated by HTs). Hence, such approaches to HT detection can be based on the following principles:

- Detection of specific features of chip structure, using a signature ("finger-printing") obtained via measurement of one or more parameters of side-channels.
- Measurement of power-supply transient signal via calibration process (and further subjected to statistical characterization) for a signal, obtained from power ports of several chips.
- Generation of test vectors to maximize the activity in individual partitions of a chip, with simultaneous minimizing the activity of other segments.
- Cyclic replication of input test vectors to increase total difference in power profile between chip, which contains HTs, and HTs-free chip.
- Use of path delays for output ports (possibly together with value of leakage current) with extensive characterization of process variations.

ASSESSMENT OF I&C SYSTEMS CYBER SECURITY

The objective of this subsection is to customize the elements of gap analysis (GA), Intrusion Modes and Effects Criticality Analysis (IMECA) technique and analysis of development processes related to the developer (human), technique, and tool (HTT) to develop an approach, which can be used in analysis and assessment of safety important I&C systems cyber security.

IMECA Technique

The FMEA is a standard formalized technique used in systems reliability analysis devoted to the specification of failure modes, their sources, causes and influence on system operability. "Failure modes" means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential (that can happen) or actual (that already happened). "Effects analysis" refers to studying the consequences of those failures.

In FMEA-technique, all possible failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected.

FMEA is used during the design stage with an aim to avoid failures in future. In the next stages it is used for process control, before and during ongoing operation of the process. The purpose of the FMEA is to take actions to eliminate or reduce possible failures, starting with the highest-priority ones. It also may be used to evaluate risk management priorities for mitigating known threat-vulnerabilities.

IMECA (Intrusion Modes and Effects Criticality Analysis) is a modification of FMEA that takes into account possible intrusions to the system (Babeshko, E. et al., 2008). Since any vulnerability can become a failure if an intrusion occurs, we can use IMECA to take into account failures caused by intrusions "using" system vulnerabilities.

It should be noted that FMEA and IMECA are not the only methods for complex systems failures and risks analysis. Authors in several related papers (e.g. Babeshko, E. et al., 2008) proved that IMECA techniques is one of the most convenient and clear in analysis of industrial Supervisory Control and Data Acquisition (SCADA) systems consisting of several hardware and specific software components with different architectures. It was performed an analysis of failures and intrusions effects for software, hardware, stored data, users and a SCADA-based system as a whole. Obtained results using Intrusion Modes and Effect Analysis technique (without criticality analysis) for a real gas cleaning system that consisted of the server, workstations and Programmable Logic Controllers were generalized by the authors, and the result is presented in Table 1.

Gap Technique

One of the fundamental concepts behind the idea of the approach is the concept of gap. Before providing a definition for gap, we propose the taxonomy of the main notions used in the chapter. Such taxonomy covers the notions of process, product, intrusion, discrepancy, gap, anomaly, vulnerability and attack (see Figure 8). We outlined clearly some important attributes of a process, product and intrusion, as well as their interrelations (Kharchenko, V. et al., 2012,c). Also, the proposed taxonomy allows tracing a case of non-ideal process in product development along with possible consequences of process implementation.

The main notions in Figure 8 are process, product, and intrusion. Processes are being implemented through the development stages of I&C system life cycle model in order to produce products. Also, products can be vulnerable to intrusions of various types that can affect the product. Results of implementation of the processes (i.e., all the set of processes that led to the creation of the product) can have effects on possible consequential changes in such processes. Each process comprises activities, and, in a case of "non-ideal" process, some of them can contain discrepancies.

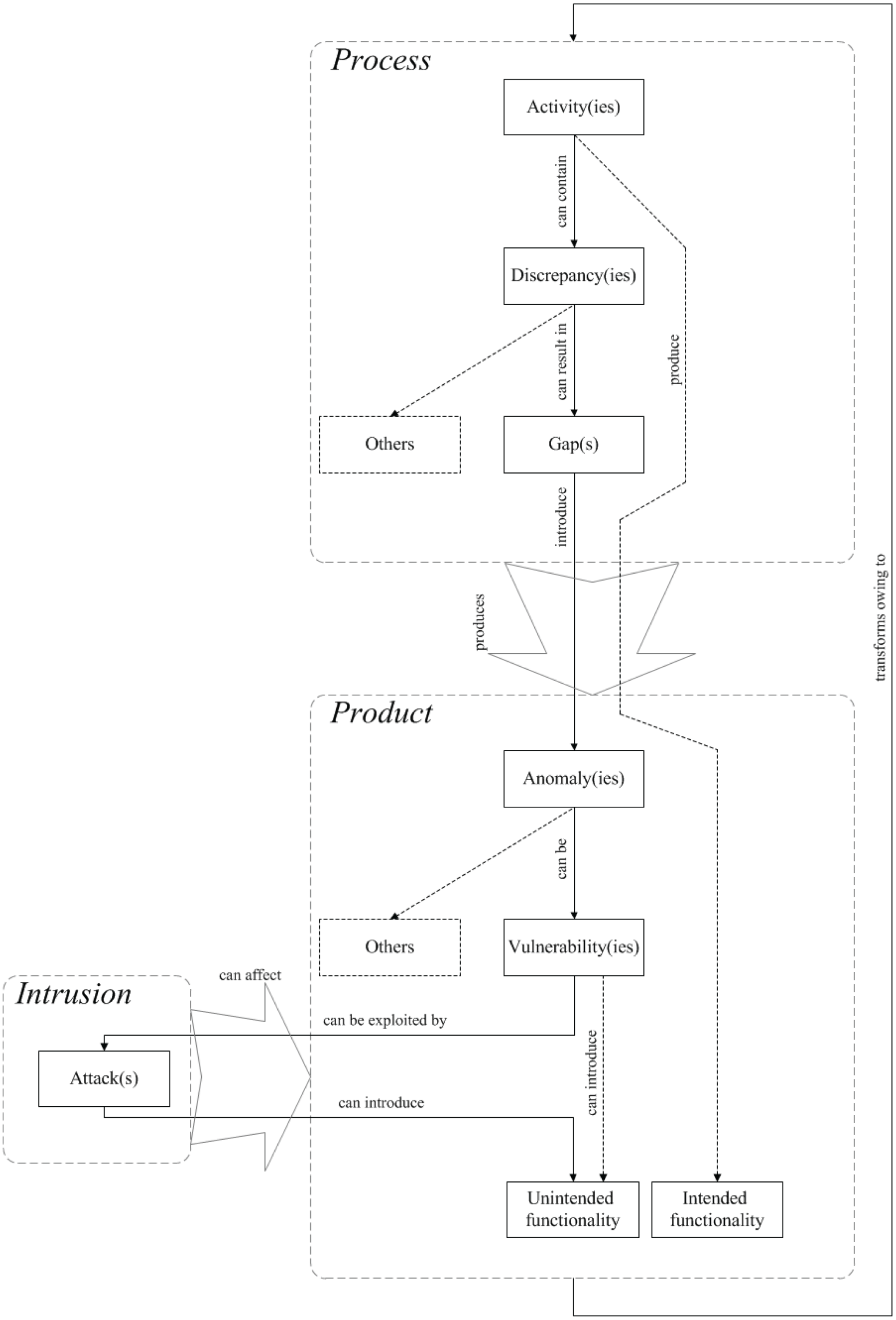
So, now we can define gap as a set of discrepancies of any single process (which can consist of a set of sub-processes) within the life cycle of I&C system that can introduce some anomalies in a product and/or cannot reveal (and eliminate) existing anomalies in a product. In particular, such anomalies can be caused by imperfection of product specification (or even representation), implementation, verification, and/or other non-compliances.

In terms of cyber security, some of the anomalies can be vulnerabilities of the product. Vulnerabilities, in turn, can be exploited by an adversary during intrusion into the product to implement

Table 1. Intrusion modes and effect analysis

Intrusion/ Attack Mode	Attack Nature	Attack Cause	Influence on Operability	Intrusion Evidence	Intrusion Effect				
					Hardware	Software	Stored Data	SCADA-based System as a Whole	User
Sniffing	passive/ active	sharing information with large community	termination	non-evident	-	-	privacy violation	SCADA-based system compromise	unauthorized access to user's data
			interruption		-	-			
			-		-	-			
System remote control	active	weak authentication	termination	evident	-	-	privacy and integrity violation	SCADA-based system incorrect operation	deny of service
			interruption		-	-			
			-	non-evident	-	incorrect operation			
OPC buffer overflow	active	OPC server without latest security patches	termination	evident	-	crash		SCADA-based system termination	
			interruption		-				
			-		-				
DoS & DDoS	active	weak system protection	termination	evident	hang	crash			
			interruption						

Figure 8. A taxonomy of used notions



an attack in order to introduce some unintended functionality into the product.

Direct relation between vulnerabilities and unintended functionality in Figure 8 denotes some possible situation, which is not covered by the scope of this chapter; such a situation may occur in the presence of hardware Trojans within the components of the product, and, hence, requires additional comprehensive analysis.

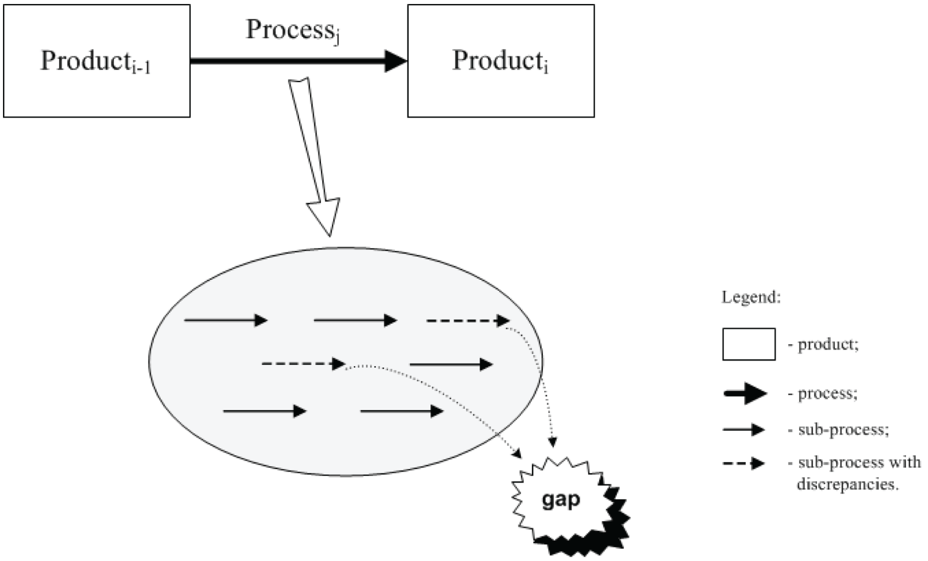
Gap-IMECA-Based Approach to Assessment of I&C System Cyber Security

Hence, we propose a process-based approach to GA, because "non-ideal" processes, which contain discrepancies, can produce various problems in the corresponding products, and the following statements are true:

1. Presence of gaps in Processj results in anomalies in Producti even if Producti-1 is "ideal."
2. Presence of anomalies within Producti-1 can be eliminated by "ideal" Processj in many cases. This may be true in case of verification and validation processes, however, it does not apply to design processes. For example, anomaly in the technical specification is not eliminated by an "ideal" direct translation process (since it may not include verification).

As an illustrative example for the proposed definition of gap, let us consider a development process within the I&C system life cycle model, where the input of Processj is represented by Producti-1, and the output (result of process implementation) – is Producti (see Figure 9). The transition from the previous product (i-1) to next one (i) is accomplished by the implementation of a prescribed process (j) by developers, using certain tools. This process can be represented as a set of sub-processes that are implemented in serial and/ or parallel ways, and each of such sub-processes may contain problems (or discrepancies towards appropriate "ideal" sub-process) due to various reasons caused by either the developer or the tool. Therefore, the problems in sub-processes lead to problems in processes, which are implemented in order to produce a new product and can result in product anomalies (Kharchenko, V. et al., 2012,d).

Figure 9. Development process in the I&C system life cycle model



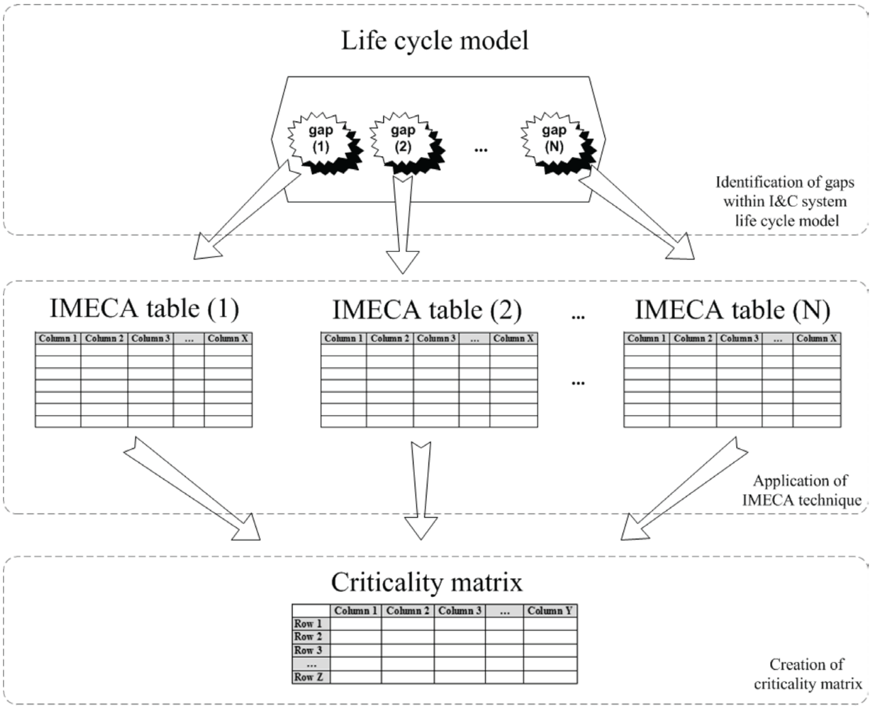
The activities, required to implement the approach, comprise several consequent steps intended for a comprehensive analysis and assessment of I&C systems. They are depicted in Figure 10.

The key idea of assessment is in the application of the process-product approach. Therefore, the life cycle model of I&C systems should include detailed representation of life cycle processes and appropriate products. Then, it is possible to identify problems (or discrepancies) within the model, i.e. gaps. In general, such gaps may reflect various aspects of the I&C system, depending on what system properties are assessed (for example, safety and security).

Hence, depending on the I&C system aspects under assessment, each gap should be represented in a form of a formal description; such a formal description should be made for a set of discrepancies identified within the gap. The IMECA technique is the most convenient, in our opinion, to perform such description: each identified gap can be represented by a single local IMECA table and each discrepancy inside the gap can be represented by a single row in that local IMECA table. In this way, complete traceability of life cycle processes, appropriate products and inherent properties of corresponding discrepancies can be achieved. As a result, the number of local IMECA tables would correspond to the number of identified gaps, and the number of rows within each local IMECA table would correspond to the number of identified discrepancies within the appropriate gap.

After completing the appropriate columns, for example on the basis of expert assessment, for all local IMECA tables, each gap is represented by a set of discrepancies with appropriate numerical values. Data within each row of local IMECA tables reveal, in explicit form, the weaknesses of the I&C system aspect under assessment: for example, in terms of safety – system faults and failures, in terms of security – intrusion probability and severity.

Figure 10. The principal stages of I&C system assessment



Further, in order to implement the approach, the following cases are possible, depending on the scope of the assessment:

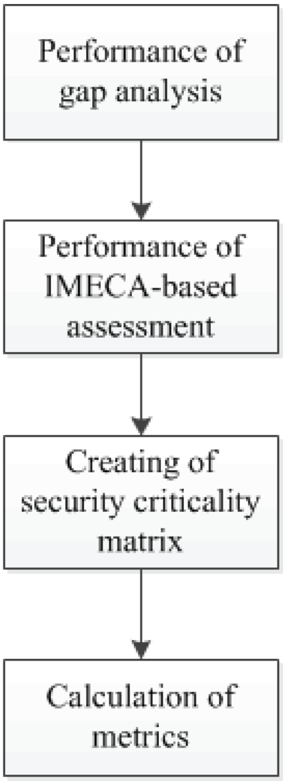
1. Assessment of the I&C system as a whole. Then, a set of particular IMECA tables (which represent all the identified gaps by a set of discrepancies) should be integrated into the single global IMECA table that reflects the whole system. In this case, each row of the global IMECA table forms the basis for creating a global criticality matrix, which can be used in cyber security assurance process.
2. Assessment of particular (sub-)systems within the I&C system. In this case, it is possible to create an appropriate set of local criticality matrixes that correspond to certain (sub-)systems, based on a set of local IMECA tables.

So, proposed gap-and-IMECA-based approach to assessment can be expressed in the consequence of actions (see also Figure 11) listed below.

Step 1: Performance of GA: identification of security gaps lists for all the components (or modules) of I&C system, being assessed, during each life cycle stage. Such lists should include both process gaps (in terms of discrepancies) and product cyber security gaps (in terms of vulnerabilities).

Step 2(a): Performance of IMECA-based assessment: determination of an appropriate set of vulnerabilities for each identified during GA process gap, security gap and possible scenarios to exploit the vulnerabilities. So, for each identified discrepancy or vulnerability, there should be created local IMECA table that reflects: attack mode, attack nature, attack cause, occurrence probability, effect severity, and type of effects. In this way each gap is being represented by one or several rows in a local IMECA table.

Figure 11. Proposed approach to assurance of cyber security


Performance of gap analysis
Performance of IMECA-based assessment
Creating of security criticality matrix
Calculation of metrics

Step 2(b): Assessment of appropriate columns (occurrence probability and effect severity) in each particular IMECA table, for example, on the basis of expert evaluation. Then, each row of such a local IMECA table represents security weaknesses, which should be analyzed further in context of the whole I&C system.

Step 3: Creating of security criticality matrix to analyze the cyber security risks of I&C system components during different stages. Each row in local IMECA tables forms the basis for creation of security criticality matrix, which reveals the weaknesses of appropriate components in a visual form. The highest cyber security risk corresponds to the highest row in security criticality matrix.

Step 4: Calculation of metrics in order to choose the optimal set of applicable security countermeasures.

In order to illustrate IMECA-based assessment, we present results for attacks modes possible during operation and maintenance stage of FPGA-based I&C system (see Table 2).

Basing on the set of local security criticality matrixes derived as a result of assessment, we can propose the following rule for integration of local security criticality matrixes into a global one in order to assess the whole I&C system:

$$e_{yz}^{G} = \bigcup_{k=1}^{n} e_{yz}^{L_k} \ , \qquad (1)$$

where e^{G} is an element of the global criticality matrix, e^{L_k} is the corresponding element of the k-th local criticality matrix, and n is the total number of local criticality matrixes (equal to total number of gaps).

Moreover, the scales for the numerical values of a discrepancy (for example, its probability and severity) for local criticality matrixes can be set to the same value in order to eliminate the necessity of additional analysis during the creation of a global criticality matrix.

In both cases, the highest risk of the selected assessment aspect corresponds to the highest row in the criticality matrix. In a case of independent gaps and discrepancies, the total risk of R can be calculated using the following equation:

$$R = \sum_{i=1}^{n}\sum_{j=1}^{m} p_{ij} D_{ij} \ , \qquad (2)$$

where *n* is the total number of gaps, m is the total number of rows in the IMECA table, *p* is the occurrence probability, and *D* is the corresponding damage.

Furthermore, the criticality matrix can be extended to be *K*-dimensional (where *K*>2) that allows us to consider, for example, the amount

Table 2. Results of IMECA for FPGA attacks

Row Number	Gap in Stage of	Attack Mode	Attack Nature	Attack Cause	Occurrence Probability	Effect Severity	Type of Effects
1	Operation	Black Box Attack	Active	Simple logic of electronic design	Very low	Very low	Reverse engineering of logic by adversary
2	Operation	Readback Attack	Active	Absence of chip security bit and/ or availability of physical access to chip interface	Moderate	High	Obtaining of secret information by adversary
3	Operation	Cloning Attack	Active	Storing of decoded configuration	Moderate	High	Obtaining of configuration data by adversary
4	Operation	Physical Attack	Active	Absence of monitoring of parameters (voltage, temperature, clock) of environment and chip	Low	Moderate	Obtaining of information concerning patented algorithms by adversary
5	Operation	Side-Channel Attack	Active	Correlation of measurable parameters with its function	High	High	Leak of undesirable information

of time required to implement the appropriate countermeasures for the assessed I&C system.

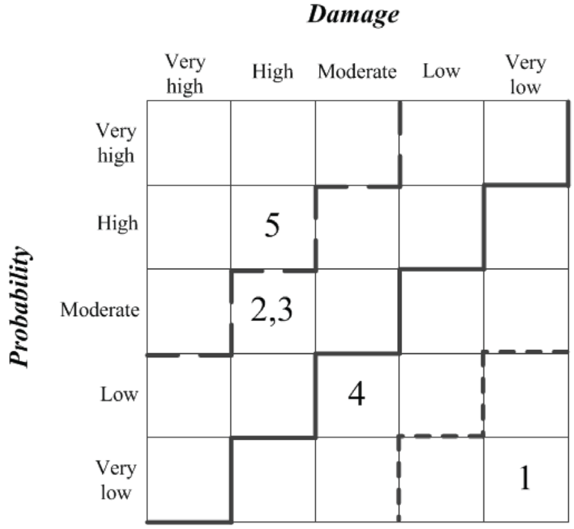
For example, during the assessment of security, the prioritization of vulnerabilities identified on the basis of process-product approach, should be performed according to their criticality and severity, representing their corresponding stages in the cyber security assurance of the given I&C system. The main goal of this step is to identify the most critical security problems within the given set. Prioritization may require the creation of a criticality matrix, where each vulnerability is represented within single rows. In such cases, it is possible to manage the security risks of the whole I&C system via changing the positions of the appropriate rows within the matrix (the smallest row number in the matrix corresponds to the smallest risk of occurrence).

During the performance of GA, the identification of discrepancies (and the corresponding vulnerabilities in case of security assessment), can be implemented via separate detection/analysis of problems caused by human factors, techniques and tools, taking into account the influence of the development environment.

Then, after all identified vulnerabilities are prioritized, it is possible to assure security of the I&C system by implementing of appropriate countermeasures. Such countermeasures should be selected on the basis of their effectiveness (also, in context of assured coverage), technical feasibility, and cost-effectiveness. But there is an inevitable trade-off between a set of identified vulnerabilities and a minimal number of appropriate countermeasures, which allows us to eliminate vulnerabilities or to make them difficult to be exploited by an adversary. The problem of choosing such appropriate countermeasures is an optimization problem and is still challenging.

Security criticality matrix is depicted in Figure 12. Each of the numbers inside the matrix represents an appropriate row number of IMECA table. Figure 12 also represents several cases of criticality diagonal for the matrix; depending on the case, possible acceptable values of risks are below the certain diagonal.

Figure 12. Criticality matrix and several possible criticality diagonals



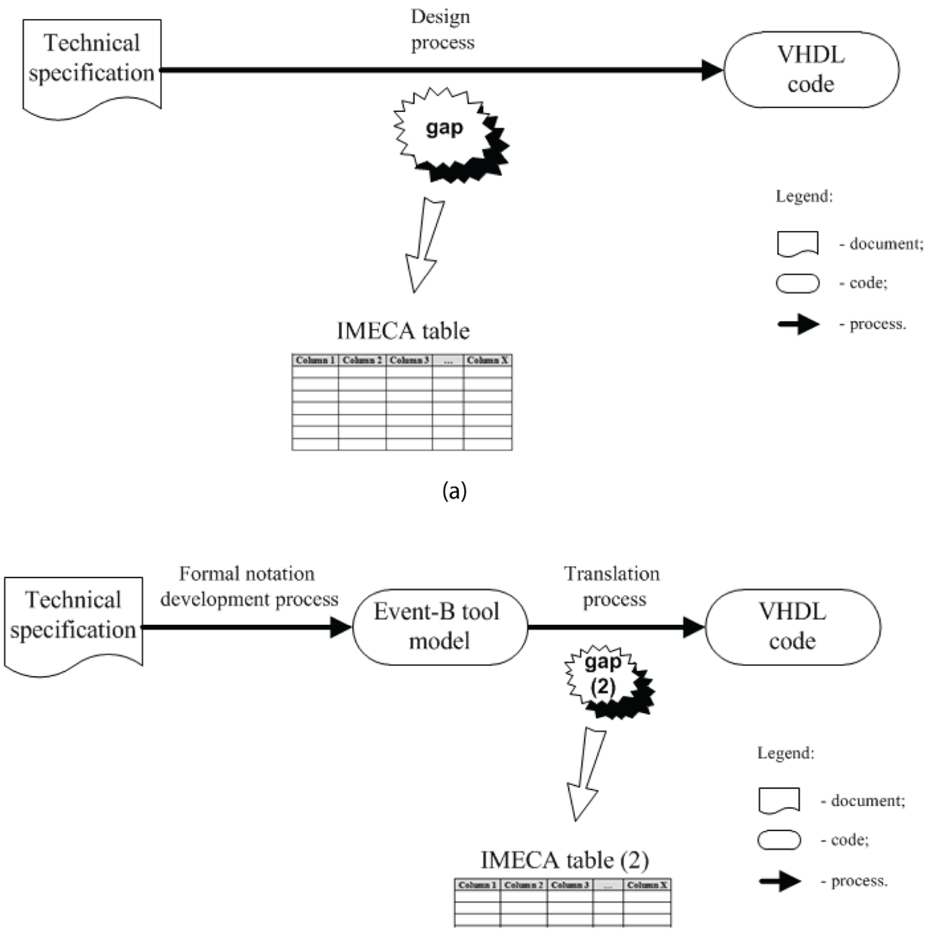
Gap-IMECA-Oriented Assessment of FPGA-Based I&C Systems

As an illustrative example for the proposed approach, consider a typical development process for a VHDL code, implemented by a developer (see Figure 13a) of FPGA-based safety important I&C system.

The input to the process is represented by a technical specification document (containing the comprehensive description of the object being developed), and the result is the VHDL code (development object). In such a case the possible discrepancies can be caused by design faults, developer's errors, and/or errors in appropriate procedures intended for the developer. Moreover, during the subsequent stages of the overall development process, existing problems in the product can be either eliminated or multiplied. Then, it is possible to represent the identified set of the process' discrepancies (or single gap) in a form of IMECA-based table, where each row corresponds to a discrepancy within the process.

Such a complex gap can be eliminated, for example, via the implementation of another development process (see Figure 13b), which includes

Figure 13. Development processes for VHDL code



(a)

(b)

three entities: technical specifications, an Event-B tool model (a form of technical specification representation in terms of a tool that is understandable to developer and can automatically be translated into a VHDL code), and the VHDL code itself.

Transitions from previous entities to the next are accomplished by the execution of certain processes, namely: formal notations development process (implemented by the developer, and consisting of translation of technical specifications into a model, in terms of internal instructions of the Event-B tool, allowing the developer to mathematically prove the correctness of the resulting notation) and the translation process (implemented by special add-ons of the Event-B tool, and consisting of generating the final VHDL code on the basis of the derived model) (Abrial, J.-R., 2010).

Discrepancies in such processes can be caused by the applied tools only, since the formal notations development process is followed by the model in Event-B tool that is mathematically verifiable. Discrepancies of the translation process (or discrepancies of its sub-processes) can be caused by the Event-B tool, for example, in a case, when such tool is not fully tested or certified.

In this way, it is possible to state that we can identify the only existing gap. Moreover, such a gap can be eliminated if certified tools are applied. Thus, in the case given in Equation (2), the risk factor *R* is reduced due to the reductions in the values of parameters *n* (from 2 to 1), *m*, and p_{ij}.

ASSURANCE OF CYBER SECURITY FOR SAFETY IMPORTANT I&C SYSTEMS

The objective of this subsection is to present an approach and possible technique of assurance the required level of cyber security for safety important I&C systems.

Approach to Assurance

As a continuation of the proposed approach to assessment of I&C systems cyber security we represent here an applicable approach to assurance of cyber security, which is based on the results of gap-IMECA-oriented assessment. Such approach consists in reduction of risks to acceptable values, which, in turn, limited by the criticality diagonal of a security criticality matrix.

Appropriate security criticality matrix is depicted in Figure 14. From cyber security assurance point of view, the possible way of risk reduction is in decreasing of attacks' occurrence probability, since related damage is constant. Figure 14 represents worst-case criticality diagonal for the matrix; acceptable values of risks are below the diagonal. Cases of probability, decreasing for rows 2, 3, and 5 are denoted by dotted lines with arrows: the problem is in decreasing of the probability by the degree sufficient to move row of IMECA table below the criticality diagonal. Such decreasing of the probability can be achieved, for example, by implementation of certain countermeasures. Some of such countermeasures, partly based on results of Christiansen B., (Christiansen, B., 2006), are presented in Table 3. The choice of countermeasures of different types can be based, for example, on RG 5.71.

A problem of choice of optimal countermeasures set is discussed in the following subsection.

Choice of Optimal Countermeasures Set

Each countermeasure can affect several security characteristics simultaneously (for example, probability of successful attack, attack severity, time to recovery), so it can be described by a set {ep, eh, et}, where ep is efficiency of successful attack probability decreasing, eh is efficiency of

Figure 14. Criticality matrixes

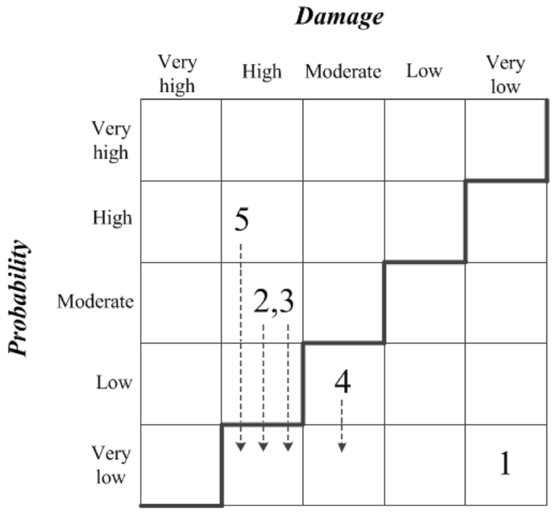


Table 3. Results of IMECA for FPGA attacks

Row Number	Attack Mode	Countermeasures
1	Black Box Attack	Complication of electronic design logic
2	Readback Attack	The use of security bit. Application of physical security controls
3	Cloning Attack	Checking of chip's internal ID before powering up an electronic design. Encoding of configuration file. Storing of configuration file within FPGA chip (requires internal power source)
4	Physical Attack	Decreasing memory retention effect. Monitoring of parameters (voltage, temperature, clock) of environment and chip
5	Side-Channel Attack	Addition of random noise in measurable parameters (or masking of information by random values). Decrease of difference in power consumption. Changing of electronic design logic

attack severity decreasing, and et is efficiency of time to recovery decreasing. The total efficiency is an integral value and can be calculated using the following equation:

$$e=ep+eh+et. \quad (3)$$

Obviously those existing security countermeasures are not completely all-purpose and can be used for certain vulnerability or a set of vulnerabilities.

Correspondence between available countermeasures and appropriate attacks can be specified in a form of matrix, where the rows represent a set of attacks possible due to I&C system's vulnerabilities detected during its security assessment, and the columns are represented by available security countermeasures and their appropriate effectiveness metrics. An example of such table is represented below (see Table 4).

After application of (3), we can represent Table 4 in a reduced form (see Table 5), which

Table 4. Effectiveness evaluation matrix for security countermeasures

Attack	Available Countermeasures									
	m_1			m_2			…	m_n		
	ep_1	eh_1	et_1	ep_2	eh_2	et_2	…	ep_n	eh_n	et_n
a_1	0	1	1	0	0	0	…	1	0	0
a_2	0	1	0	1	0	0	…	0	0	0
…	…	…	…	…	…	…	…	…	…	…
a_k	1	1	0	0	1	0	…	1	1	0

Table 5. Integral evaluation of security countermeasures effectiveness

Attack	Available countermeasures						
	m_1		m_2		…	m_n	
	e_1	c_1	e_2	c_2	…	e_n	c_n
a_1	2	$c_{1,1}$	0	$c_{1,2}$	…	1	$c_{1,n}$
a_2	1	$c_{2,1}$	1	$c_{2,2}$	…	0	$c_{2,n}$
…	…	…	…	…	…	…	…
a_k	2	$c_{k,1}$	1	$c_{k,2}$	…	1	$c_{k,n}$

includes integral effectiveness of the countermeasures compared to each of the possible attacks.

Application of the specific security countermeasure requires certain costs. Hence, such costs will depend on the chosen countermeasure and appropriate attack type. Costs of certain countermeasure application can be defined in a form of table, as well as integral effectiveness (see Table 5).

A problem of optimal choice of security countermeasures can be solved in two ways:

1. Minimization of costs associated with purchasing and implementation of countermeasures in order to decrease the criticality for all possible attack types down to some predefined level.
2. Maximal possible decreasing of attacks criticality within the predefined limits for appropriate costs.

First problem is actual for I&C systems of critical application and can be formulated in the following way:

$$f\left(x\right)=\sum_{i=1}^{m}\sum_{j=1}^{n}c_{i,j}x_{i,j}=cx\rightarrow\min,\ \ x\in D \quad (4)$$

$$D=\left\{x\in R^{mn}\mid\sum_{j=1}^{n}e_{i,j}\cdot x_{i,j}+d_i>CR,\ i\in\overline{1,m};\ \ x_{i,j}\in\left\{0,1\right\}\right\} \quad (5)$$

where d_i is initial level of i-th attack type criticality; *CR* is a number that defines criticality diagonal; $e_{i,j}$ is effectiveness of j-th countermeasure application to i-th attack type; $c_{i,j}$ is costs of j-th countermeasure application to decrease criticality of i-th attack type.

Initial level of i-th attack type criticality is set with some value, as well as criticality diagonal, and is defined by a position within criticality matrix in according to qualitative evaluation of its appearance probability, effect severity and recovery time.

Required variables $x_{i,j}$ can be calculated in the following way:

$$x_{i,j} = \left[\begin{array}{l} 1,\ if\ \ j-th\ countermeasure\ is\ applied \\ \quad to\ decrease\ criticality\ of\ i-th\ attack\ type; \\ 0,\ if\ \ j-th\ countermeasure\ is\ not\ applied \\ \quad to\ decrease\ criticality\ of\ i-th\ attack\ type. \end{array}\right.$$

Such a problem is one of the combinatorial problems class, when optimization function is defined at finite set with elements represented by samples of *m* x *n* elements (*n* countermeasures, which can be applied for each of *m* possible attack types). However, in some cases, values of unknown variables $x_{i,j}$ can be determined within the set of nonnegative integer numbers $x_{i,j} \in Z^{+}$. It is appropriate, for example, when redundancy of elements is used to decrease the criticality.

In this case value of $x_{i,j}$ defines redundancy rate; appropriately, costs of such countermeasures application $c_{i,j}$ increases with multiply number. In some cases, the redundancy rate can be limited in an explicit way.

In such definition, the optimization problem for choice of security countermeasures falls into wide class of integer problems of linear programming. Nevertheless, it can be reduced to a subclass of combinatorial problems. In this case, different redundancy rate should be represented as separate method containing estimation of costs and effectiveness that depends on the rate.

According to (7.4) and (7.5), global optimization of objective function *f(x)*, can be reduced to phased optimization. Hence, optimal minimization of costs, associated with security countermeasures application, is additive object function for which the effect of a such decision for a single attack type is corresponding (6).

$$f\left(x_{1,1},\ldots,x_{1,n},\ldots,x_{2,n},x_{i,1},\ldots,x_{i,n},x_{m,1},\ldots,x_{m,n}\right) = \sum_{i=1}^{m} f_{i}\left(x_{i,j}\right) \tag{6}$$

To solve this problem it is appropriate to use a method of dynamical programming.

Second problem requires formulating of object function. It is possible using mean arithmetical value of noncriticality, which, in turn, can additionally be weighted depending on the importance of the attack type. Initial generalized level of noncriticality of I&C system can be defined using Equation (7) and (7.8) to take into account weights of the attack:

$$NCR = \frac{\sum_{i=1}^{m} d_{i}}{m}, \tag{7}$$

$$NCR = \sum_{i=1}^{m} a_{i} d_{i},\ \sum_{i=1}^{m} a_{i} = 1. \tag{8}$$

Then, a problem of criticality decreasing with specified limitations of costs can be formulated in the following way:

$$f\left(x\right) = \sum_{i=1}^{m} a_{i} \sum_{j=1}^{n} e_{i,j} x_{i,j} + d_{i} \to \max,\ \sum_{i=1}^{m} a_{i} = 1,\ x \in D \tag{9}$$

$$D = \left\{ x \in R^{mn} \mid \sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j} x_{i,j} \le C_{\max};\ x_{i,j} \in \left\{0,1\right\} \right\} \tag{10}$$

where d_i is an initial level of noncriticality for *i*-th attack type; C_{max} is maximal acceptable costs for all the countermeasures applied to decrease the criticality of attacks; $e_{i,j}$ is an effectiveness of *j*-th countermeasure application towards *i*-th attack type; $c_{i,j}$ is costs of j-th countermeasure application in order to decrease criticality of *i*-th attack; a_i is a weighting coefficient of *i*-th attack.

To solve the formulated problem, one of discrete programming methods can be used, for example, branch and bound method.

Solution and Recommendations

A problem of security assessment and assurance for safety important I&C systems is still challenging due to the fact that such systems consist of interconnected complex components with different functions and different nature; moreover, the majority of modern I&C systems are being FPGA-based, hence, it is impossible to perform their assessment without consideration of all the special features for all the technologies used.

To assure cyber security of safety important I&C systems, as well as to decrease a probability of vulnerabilities exploitation and appearance of security breaches, a cyber security assessment approach is proposed. This approach implies identification of all possible discrepancies, on the basis of product and life cycle processes, and their assessment via application of IMECA technique. The proposed approach is based on both gap conception and IMECA technique. Such an approach is applicable in assessment of various aspects of safety important I&C systems, since it considers process-product model to reveal all the process discrepancies that can potentially result in product anomalies.

Next important steps of research and development activities, related to assurance of security for safety important I&C systems, may be connected with creation and implementation of tool-based support for the proposed approach, taking into account results of qualitative and quantitative assessment.

FUTURE RESEARCH DIRECTIONS

The future research directions are the following:

- Development of a tool that supports gap-IMECA-based approach.
- Implementation of tool-based calculation of metrics used in choosing the optimal set of applicable security countermeasures.

CONCLUSION

The assessment of safety important I&C systems security, as well as further assurance of such attribute, is very important and challenging problem, in terms of both regulations and their consequent implementation. This chapter discusses some problems related to assessment of security aspects of safety critical, including FPGA-based, I&C systems.

Proposed here main elements of the approach to cyber security assurance allows decreasing a probability of vulnerabilities exploitation and appearance of security weaknesses in safety important I&C systems. Thus, approach implies conducting of gap analysis, based on identification of all possible vulnerabilities, on the basis of product and life cycle processes, and their assessment via application of IMECA technique.

The proposed approach and technique were applied to cyber security assessment of RadICS FPGA-based I&C platform developed by Research and Production Corporation Radiy. Furthermore, gap-and-IMECA-based technique was applied in development of a company standard in Research and Production Corporation Radiy that is harmonized with international standards. This standard is used during implementation of development and verification activities for safety-critical I&C systems for nuclear power plants.

REFERENCES

Abrial, J.-R. (2010). *Modeling in event-B*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9781139195881

ANSI/ISA-99.00.01-2007. (2007). *Security for industrial automation and control systems: Terminology, concepts, and models*.

ANSI/ISA-99.00.02-2007. (2007). *Establishing an industrial automation and control systems security program*.

ANSI/ISA-99.00.03-2007. (2007). *Operating an industrial automation and control systems security program*.

ANSI/ISA-99.00.04-2007. (2007). *Specific security requirements for industrial automation and control systems*.

ANSI/ISA-99.02.01-2009. (2009). *Security for industrial automation and control systems: Establishing an industrial automation and control systems security program*.

ANSI/ISA-TR99.00.01-2007. (2007). *Security technologies for industrial automation and control systems*.

Babeshko, E., et al. (2008). Applying F(I)MEA-technique for SCADA-based industrial control systems dependability assessment and ensuring. In *Proceedings of International Conference on Dependability of Computer Systems DepCoS–RELCOMEX 2008*. Academic Press.

Badrignans, B. etal. (2011). *Security trends for FPGAS: From secured to secure reconfigurable systems*. Berlin: Springer. doi:10.1007/978-94-007-1338-3

Drimer, S. (2009). *Security for volatile FPGAs* (Technical Report N 763). Cambridge, UK: University of Cambridge Computer Laboratory.

EPRI TR1019181. (2009). *Guidelines on the use of field programmable gate arrays (FPGAs) in nuclear power plant I&C systems*. Electric Power Research Institute.

EPRI TR1022983. (2011). *Recommended approaches and design criteria for application of field programmable gate arrays in nuclear power plant I&C systems*. Electric Power Research Institute.

GAO-04-321. (2004). *Cybersecurity for critical infrastructure protection*. Washington, DC: U.S. General Accounting Office.

Grand, J. (2004). Practical secure hardware design for embedded systems. In *Proceedings of the 2004 Embedded Systems Conference*. San Francisco, CA: Academic Press.

Huffmire, T. etal. (2010). *Handbook of FPGA design security*. Berlin: Springer. doi:10.1007/978-90-481-9157-4

IAEA. (2011). *Computer security at nuclear facilities: Reference manual: Technical guidance*. Vienna, Austria: IAEA.

IEC 60880. (2006). *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions.* IEC.

IEC 61513. (2011). *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*. IEC.

IEC 62138. (2004). *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.* IEC.

IEC 62566. (2010). *Nuclear power plants – Instrumentation and control important to safety – Hardware language aspects for systems performing category A functions*. IEC.

IEC 62645. (2011). *Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems.* IEC.

ISO/IEC 27001. (2005). *Information technology – Security techniques – Information security management systems – Requirements.* ISO/IEC.

ISO/IEC 27002. (2005). *Information technology – Security techniques – Code of practice for information security management.* ISO/IEC.

ISO/IEC 17799. (2005). *Information technology – Security techniques – Code of practice for information security management*. ISO/IEC.

ISO/IEC 27000. (2009). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. ISO/IEC.

ISO/IEC 27004. (2009). *Information technology – Security techniques – Information security management – Measurement.* ISO/IEC.

ISO/IEC 15408. (2009). *Information technology – Security techniques – Evaluation criteria for IT security*. ISO/IEC.

ISO/IEC 27003. (2010). *Information technology – Security techniques – Information security management system implementation guidance.* ISO/IEC.

ISO/IEC 27005. (2011). *Information technology – Security techniques – Information security risk management.* ISO/IEC.

ISO/IEC 27006. (2011). *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.* ISO/IEC.

ISO/IEC 27007. (2011). *Information technology – Security techniques – Guidelines for information security management systems auditing*. ISO/IEC.

ISO/IEC 27008. (2011). *Information technology – Security techniques – Guidelines for auditors on information security management systems controls.* ISO/IEC.

Karry, R., et al. (2010, October). Trustworthy hardware: Identifying and classifying hardware trojans. *Computer Magazine*, 39-46. Christiansen, B. (2006). *Active FPGA security through decoy circuits*. (MS Thesis). Air Force Institute of Technology.

Kharchenko, V., et al. (2011). Critical infrastructures safety: Mathematical and engineering methods of analysis and assurance. Department of Education and Science of Ukraine, National Aerospace University named after N. Zhukovsky KhAI. IEC 61508: Ed. 2. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems.* IEC.

Kharchenko, V., et al. (2012a). Cyber security of FPGA-based NPP I&C systems: Challenges and solutions. In *Proceeding of the 8th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies* (NPIC & HMIT 2012). San Diego, CA: NPIC & HMIT.

Kharchenko, V. et al. (2012b). GAP- and HTT-based analysis of safety-critical systems. *Radioelectronic and Computer Systems*, *7*(59), 198–204.

Kharchenko, V. et al. (2012c). Gap-and-IMECA-based assessment of I&C systems cyber security. *Advances in Intelligent and soft. Computing*, *170*, 149–164.

Kharchenko, V., et al. (2012d). Cyber security lifecycle and assessment technique for FPGA-based I&C systems. In *Proceeding of IEEE East-West Design & Test Symposium* (EWDTS'2012). Kharkov, Ukraine: IEER.

NEI 08-09. (2010). *Cyber security plan for nuclear power reactors*. Nuclear Energy Institute.

NIST SP 800-30. (2002). *Risk management guide for information technology systems*. Washington, DC: National Institute of Standards and Technology.

NIST SP 800-53. (2009). *Recommended security controls for federal information systems and organizations*. Washington, DC: National Institute of Standards and Technology.

NUREG/CR-7006. (2010). *Review guidelines for field-programmable gate arrays in nuclear power plant safety systems*. Washington, DC: U.S. Nuclear Regulatory Commission.

Ravi, S. etal. (2004). Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems*, *3*(3), 461–491. doi:10.1145/1015047.1015049

RG 5.71. (2010). *Cyber security programs for nuclear facilities.* Washington, DC: U.S. Nuclear Regulatory Commission.

Sadeghi, A.-R. etal. (2011). *Towards hardware-intrinsic security: Foundations and practice*. Berlin: Springer.

Tehranipoor, M., et al. (2010). A survey of hardware trojan taxonomy and detection. In *Proceedings of IEEE Design & Test of Computers*. IEEE.

ADDITIONAL READING

Badrignans, B. etal. (2011). *Security Trends for FPGAS: From Secured to Secure Reconfigurable Systems*. Springer. doi:10.1007/978-94-007-1338-3

Chakraborty, R., et al. (2009). *Hardware Trojan: Threats and Emerging Solutions* / Proceedings of High Level Design Validation and Test Workshop (HLDVT 2009). San Francisco, CA. November 4-6, 2009. Pp.166-171.

Gorbenko, A. etal. (2006). In M. Butler, C. Jones, A. Romanovsky, & E. Trubitsyna (Eds.), *F(I) MEA-Technique of Web-services Analysis and Dependability Ensuring / Rigorous Development of Complex Fault-Tolerant Systems. LNCS4157* (pp. 153–167). Springer. doi:10.1007/11916246_8

Kastner, R., et al. (2008). *Threats and Challenges in Reconfigurable Hardware Security* / International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA'08). – Las Vegas, NV. July 2008. Pp.334-345.

Maggioni, M. (2010). Trojan-free FPGA circuits using ECC-based functional trust-checking. Thesis, Politecnico di Milano. 141p.

NIST FIPS PUB 140-2:2001, *Security requirements for cryptographic modules*, National Institute of Standards and Technology, (2001).

Tehranipoor, M. (2011). *Introduction to Hardware Security and Trust*. Springer.

KEY TERMS AND DEFINITIONS

Identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Regulatory Requirement: Requirement which is established by National Regulatory Authority (authority designated by government for regulatory purposes for safety assurance).

Risk: The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring.

Security: Avoidance of dangerous situation due to malicious threats.

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Chapter 8
Overall Instrumentation and Control Systems

Yuri Rozen
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Grygoriy Gromov
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Vladislav Inyushev
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

ABSTRACT

Chapter 8 considers design principles of Overall Instrumentation and Control (OI&C) systems implemented at Ukrainian NPPs. The first section provides brief information on controlled objects—power units with reactors WWER, which are operated at Ukrainian NPPs. The main principles and features for modernization of OI&C systems and their components in NPPs in Ukraine that were generated in 2000-2011 are further provided. The third section is dedicated to the architecture of OI&C systems that control technological processes on these power units. After that, the central part of this architecture, a group of the most closely connected individual Instrumentation and Control (further, I&C) systems, for which the general term "reactor control and protection system" is used in Ukraine and Russia, is considered in detail. The purpose, composition, and structure of a modernized reactor control and protection system that are implemented at Ukrainian NPPs with WWER reactors are provided.

INTRODUCTION

Ukrainian and Russian specialists of different branches of industry, including atomic energy, widely use the term "Automated Process Control System" (APCS). In regulation NP, 2008 an implicitly close term "automated monitoring and control system of power unit technological processes" that should provide remote and / or automatic control of technological processes and safety systems, automatic protection of systems, equipment and power unit as a whole, and also monitor that limits of its safe operation are not exceeded, is introduced. In international standards (IEC, 2011), the concept of overall instrumentation and control (OI&C) system that denotes a complete set of all individual instrumentation and control systems of a power unit and covers normal opera-

DOI: 10.4018/978-1-4666-5133-3.ch008

tion systems as well as safety systems, is used. In these terms, OI&C system can be considered as an English equivalent of APCS.

In the section that begins this chapter, a short description of a controlled object required for understanding of issues of automatic monitoring and control of power unit technological processes executed by the OI&C system is given. Direct description is premised with consideration of the modernization concept for the OI&C system adopted in Ukraine, which has been almost implemented at Ukrainian NPPs. The stages of modernization of I&C systems of Ukrainian NPPs are described. The first stage (1993-2000) was characterized by use of systems designed by foreign (including USA) companies. The second stage (2001-2012) was characterized by use of systems designed by Ukrainian companies. The modernization strategy is analyzed in two aspects: the strategy of operators and the strategy of I&C designers.

Figure 1 shows graphic symbols and notation conventions used in this and further chapters.

BACKGROUND

The designs of nuclear power units with reactors WWER (water-cooled water-moderated power reactors) operated at NPPs of Ukraine were developed in the 1970-s in the USSR by the Kurchatov Institute of Atomic Energy (now – Russian Scientific Center "Kurchatov Institute"), the Design Bureau Gidropress is the Chief Designer of reactor facilities equipped with reactors WWER.

First reactor facilities with nuclear reactors WWER-1000 (with nominal electrical power 1000 MW) were models V-302 and V-338 (operated at South-Ukrainian NPP units 1 and 2, respectively). Serial (typical) model V-320 of the unit was first implemented in Ukraine in 1984 at Zaporozhe NPP unit 1. As it was mentioned in IAEA, 1997, "in general, 320 design conforms to standards used in the world practice for safety systems and safety important systems. A basic concept of defense-in-depth for safety assurance is implemented in general development criteria, including use of redundancy, diversity, independence and security."

In 1984-1989, in Ukraine 8 power units with B-320 reactor facilities were produced, in 1995 – one more power unit. The construction of two power units (Khmelnitsky NPP unit 2 and Rovno NPP unit 4) started in 1984, was stopped after the accident at Chernobyl NPP and continued only after 13 years. Both units were completely constructed and commissioned in 2004. In total, at 4 Ukrainian NPPs 13 power units with reactors WWER-1000 (11 of them have serial V-320 reactor facilities) are operated. In addition, two power units Rovno NPP units 1 and 2) with reactors WWER-440 (with nominal electrical power 440 MW) are operating now. The design lifetime of units WWER-440 (30 years) expired in 2010-2011 and after required measured were taken, it was extended for 20 years. Power units with other types of nuclear reactors are not operated in Ukraine (RBMK reactors used at the Chernobyl NPP are now decommissioned).

Russia currently operates 16 power units with reactors WWER-1000 and WWER-440. Similar power units are used in China, India, Finland, Czech Republic, Slovakia, Hungary, Armenia, Bulgaria, and Iran. New power units with reactors WWER in Russia, Ukraine, China, India, and Armenia (where reactors of such types have already been operated) and also in Belorussia, Vietnam, Nigeria, Turkey are at different stages of construction.

The main literature devoted to reactor facilities of operating power units is published (in Russian) in a series of the designers' monographs "Construction of reactor facilities WWER for NPPs," which include information on reactors WWER-440 (Bessalov, 2004), WWER-1000 (Rezepov, 2004), control rod drives (Nikituk, 2004) and other equipment used in them. Different aspects of safety assurance of nuclear power plants are considered in the books Nosovsky,

Figure 1. Symbols and designations

S S	Sensors (measurement field devices)
A A	Actuators (actuating field devices)
380	Elements of actuators remote control
	Mnemonic diagrams
	Visual alarms
🔊	Audio alarms
380	Digital indicators
	Analog indicators / recorders
	Quasi-analog indicators
🖨	Printers
	Manual control devices (keys, keyboard, set-points device, mode switches, etc.)
	Recording on removable media device (Winchester, flash memory)
WS	Workstations of personnel
HMI	Human-machine interface devices (computers for view, storage, registration of data)
■	Built-in panel computer
🖥	Liquid-crystal monitors, plasma-panel monitors
a	Designation signals ERP, PRP1, PRP2
b	Designation signals Pw ≥ ERP«Pw», T ≤ ERP«T», Pw ≥ PRP1«Pw», T ≤ PRP1«T», Pw ≥ PRP2«Pw», T ≤ PRP2«T»
g	Designation signals Pw ≥ 25%, Pw ≥ 75%, Pw ≥ ULAR «Pw»
e	Designation signals of violations of specified operational limits of a local energy release, reserve before a boiling crisis on a surface of fuel elements and a coolant temperature at the output of fuel assemblies
NFMS	Neutron flux monitoring system
E&PRPS	Emergency and preventive reactor protection system
RPW CUL & APPS	Reactor power control, unloading, limitation and accelerated preventive protection system
RG & ICS	Rod group and individual control system
PSS	Power supply system of control rod drivers
BRS	Boron regulation system
IRMS	In-core reactor monitoring system
RMCS	Refueling machine control system
CIS	Computer information system and safety parameters display system
TCS	Turbine control system
MCR	Main control room
ECR	Emergency control room
LOC	Room of personnel, which maintain reactor control and protection system

2006; Samoilov, 1989; Ostreikovsky & Shviraev, 2008; Makhutov, 2009, etc. Description of reactor structures and equipment, including automation systems, is given in the encyclopedia Adamov, 2005. In more detail I&C systems of these reactors are described in the books Plutinsky & Pogorelov, 1983, and Yastrebenetsky, 2004.

Among English publications devoted to I&C systems used for monitoring and control of these reactor facilities of NPPs, Chapter 43 «I&C principles for PWR plants in the Russian Federation» in the IAEA, 1999 guidebook (author of this chapter – V. Neboyan) should be mentioned first.

BRIEF INFORMATION ON POWER UNITS WITH REACTORS WWER

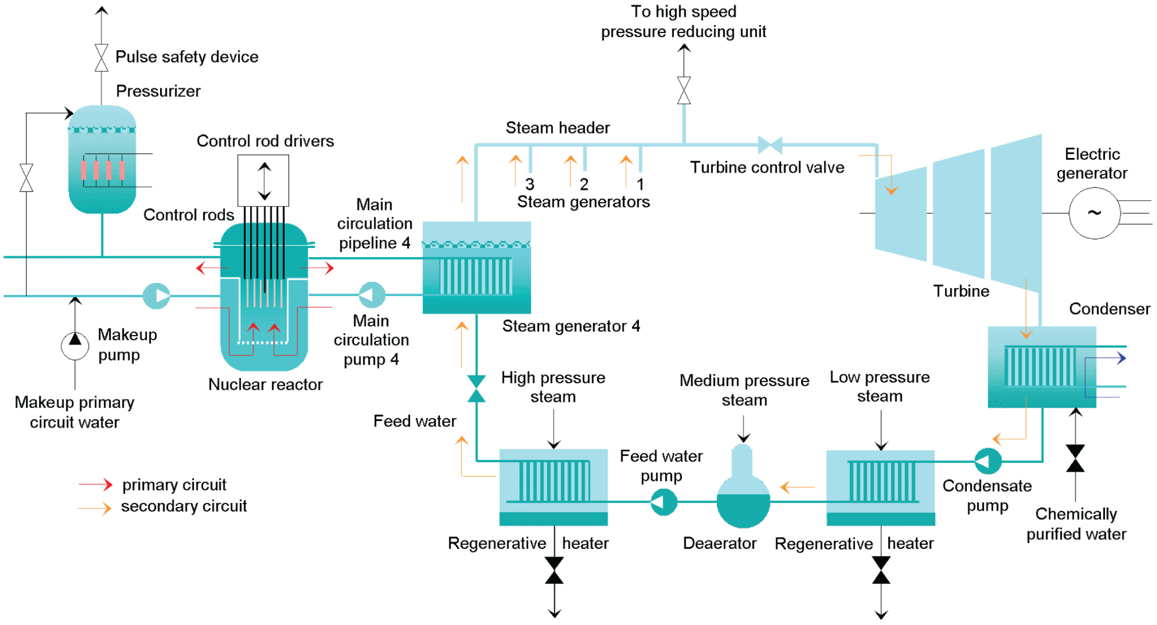
Reactors WWER include Pressurized Water Reactors (PWR), being the most widespread type of reactors in world atomic engineering (total capacity of PWR exceeds half of the world one).

Figure 2 shows a simplified technological scheme of a power unit with WWER-1000 reactor. The main technological equipment of a power unit is nuclear reactor, main circulation pumps (1…4), pressurizer, steam generators (1…4), steam header, steam turbine, condenser, regenerative heaters, deaerator, feedwater pumps, electric generator.

Primary circuit is formed by: nuclear reactor; four circulation loops, each of which is formed by a steam generator, main circulation pump and piping; steam pressure compensator (pressurizer); pressure relief tank, make-up blowdown systems, boron regulation systems, steam generator emergency power supply systems and other systems and equipment (not shown in Figure 2), providing normal operation and safety of nuclear facility.

WWER-1000 is a cylindrical vessel, consisting of a shell and removable upper block with a cover. Fuel is low-enriched uranium dioxide. As the primary coolant circuit and neutron moderator, demineralized water with a boron solution,

Figure 2. Simplified technological scheme of power unit with WWER-1000



whose which concentration can be changed during operation, is used.

The core, in which heat transfer from nuclear fuel to the coolant is provided, is located in the reactor shell. 163 fuel assemblies, each of which consists of 312 fuel elements, generating heat energy, which are placed in a protective cover of hexahedral form, are located in the core. Nuclear fuel in the form of pellets of enriched uranium-235 is placed in sealed tubes of zirconium alloy, protecting fresh fuel and burnup fractions from contact with the coolant. Some fuel assemblies have specific channels, in which rods of the material that actively absorbs neutrons can move. Position of absorbing rods in the core defines neutron flux density that allows regulating reactor power due to a controlled transfer of absorbing rods. In WWER-1000 reactors a group (cluster) of 18 absorbing rods is transferred by one actuator, forming control rod (CR). Besides transfer (lifting and drop) of the cluster, control rod drive also provides shutdown by CR moving from the upper to lower position, holding in any of intermediate positions by height of the core and drop of CR to the lower dead stop, providing a rapid change of neutron power by a protection command (including reactor emergency shutdown). Change of reactor power can be also executed by change of boric acid solution concentration in the primary coolant (boron regulation system).

Primary coolant from an output of the reactor core transfers through a “hot leg” of each main circulation piping into a heat exchanger of a proper steam generator, from which output through a “cold leg” of the same piping return to the core. During reactor operation circulation of the primary coolant is provided by four main circulation pumps.

Creation of primary coolant pressure, required for reactor start-up, maintaining of pressure during power operation and compensation of pressure deviations during coolant temperature variations, is provided by the pressurizer, connected to the hot leg of one of primary loops. This coolant temperature is maintained at the level that conforms to steam saturation temperature under required primary circuit pressure. Pressure decrease is compensated by connection of the electric heating unit, inbuilt in the pressurizer, pressure increase – injection of the coolant from the cold leg of circulation loop into the steam room. In emergencies, in cabinet of pressure increase, steam from the pressurizer is discharged into the pressure relief tank trough a pulse safety device.

Steam generator has a horizontally located cylindrical shell and a heat exchanger whose surface is located lower than the nominal level of feedwater. As a result of heat exchange between the primary coolant and feedwater, dry saturated steam is produced for the turbine. Heat-exchange surface in each steam generator is a boundary between the primary and secondary reactor circuits.

Secondary circuit formed by:

- The space between the shell and the outer surface of the heat exchanger of each steam generator.
- Blowdown subsystem and impulse protective equipment of steam generators.
- Steam lines from steam generators and steam header.
- Turbine set, consisting of a steam turbine, regenerative heaters of high and low pressure, moisture separators (not shown in Figure 2), condenser and condensate pumps.
- Feedwater pumps, regenerative heaters, deaerator, steam lines and piping of high and low pressure, including fast acting pressure reducing stations.

In operating mode waste steam is discharged from a turbine into a condenser. Cooling of the condenser is executed by water pumping from an ultimate heat sink through a heat exchanger. Condensate pumps transfers condensate to a deaerator through regenerative heaters of low pressure. Feedwater, purified from gases in the deaerator, is supplied with feedwater pumps through regenerative heaters of high pressure and in the form of steam returns to the condenser through steam lines, steam collector and turbine set. Coolant loss in the secondary circuit is compensated by supply of chemically purified water into the condenser.

PRINCIPLES I&C SYSTEMS MODERNIZATION AT NPPS IN UKRAINE

The reasons for upgrading of I&C systems at NPPs in Ukraine are as following:

- The incomplete compliance with the modern requirements on nuclear and radiation safety.
- The end of the useful life of the most types of the instruments (lifetime of many instruments is now over or close to the end (8-10 years).
- The absence of spare parts for many types of equipment because a lot of manufactures that supplied NPPs with spare parts before, ended their actions or changed direction of their work after USSR disintegration.

Let us consider the first reason in detail. This reason includes:

- Low level of reliability.
- Low quality of man-machine interface.
- Non-satisfactory diagnostics of hardware and software.
- Discrepancy to seismic requirements, to requirements of resistance to actions of environment.
- Low fire resistance.
- Absence of systems for information personnel support.
- Absence of high (general plant) level co-operated with unit level.

First stage of modernization (1993-2000) was characterized by using the systems designed by foreign companies USA (Westinghouse), Czech Republic (Skoda), Russia (Kurchatov Institute), France (SYSECA), etc. Most of these systems were safety-related.

Ukraine had no uniform strategy for I&C modernization at that time. Some of these systems had good fate and continue to operate now. This concerns first of Safety parameters display system (SPDS) for 11 Ukrainian units which operated at that time. SPDS was designed by Westinghouse (USA) together with joint USA - Ukrainian Corporation "Westron" (see Chapter 1).

Some of these systems (e.g. computer information systems designed by SYZECA were replaced during the second stage of modernization.

Ukraine did not have its own regulations related to I&C systems during that time. The Ukrainian Regulatory Authority used USSR standards and standards of the countries-designers in licensing process for these systems (Brenman, 2006).

Second stage of modernization was implemented during 2001-2011. The main peculiarities of this stage are:

- Modern computer techniques were widely used.
- New national regulatory framework was developed.
- Most I&C systems were designed and produced by Ukrainian companies.
- Modernized I&C were not only safety-related systems but safety systems as well (e.g., reactor protection systems).

The modernization strategy is analyzed in the following aspects:

- Strategy of operators (NPP or National Nuclear Energy Generating Company «Energoatom»).
- Strategy of I&C systems designers.

- The main features peculiar to the strategy of operators are the following:

    - ◦ Most modernizations take place during shutdown for refueling. This time is limited, and in some cabinets the shutdown period is insufficient for modernization. In these cabinets, modernization is implemented in 2 or 3 stages (examples: complete modernization of the unit computer information system or neutron flux monitoring system). The presence of several stages required additional activities to ensure the compatibility between modernized and non-modernized parts of the systems.
    - ◦ All I&C modernizations can be divided into pilot (modernizations implemented for the first time at NPP with specific reactor type) and replicated (modernizations implemented before at a specific NPP type in Ukraine and showed positive results). Of course, use of replicated systems is preferable in terms of safety justification and cost for acquisition of systems. The scope of licensing actions for replicated modernizations is substantially smaller than for pilots. A specific stage in the implementation of a pilot system is its trial operation with extensive support from the designer and prompt feedback from the NPP to the designer, involving analysis of all failures, faults or NPP personnel comments.
    - ◦ Most modernizations used existing technological algorithms, which were proven by long-term operation of power units in Ukraine, Russia and other countries. The algorithms were modified to include new functions, e.g. control of primary-to-secondary leakage accidents.
    - ◦ Modernizations can be related to the central part of a system or to a system as a whole, together with sensors, cables, actuators. In the beginning of this stage modernizations involved only central-part of systems. (as a rule, computer-based). In recent times, replacement of cables and sensors is included into the scope of modernizations.
    - ◦ Extensive I&C modernization took place before unit life extension. NPP paid special attention to these actions and assigned resources for unit life extension, including replacements of old I&C systems. The Regulatory Authority requested these replacements from the NPP to receive a license for unit life extension. Some of I&C systems, which were modernized to obtain approval for unit life extension, is shown in Table 1.

The main features peculiar to the strategy of designers are the following:

- Use of an aggregate of hardware, software and service apparatus called hardware-software complex (HSC) as the central part of systems (see Chapter 1)
- Ukrainian Research and production Corporation “Radiy” pioneered the application of field programmable gate array (FPGA) for performance of safety functions (reactor protection systems, engineering safety features actuation system, etc.). Since 2004, more than 40 FPGA-based systems have been installed at Ukrainian NPPs. IAEA Independent Engineering

Table 1. I&C systems that were modernized for approval of power unit life extension

Name of System	Designation	Designer
Neutron flux monitoring system	NFMS	"Impuls" (Ukraine)
Emergency and preventive reactor protection system	E&PRPS	"Radiy" (Ukraine)
Reactor power control, unloading, limitation and accelerated preventive protection system	RPw CUL & APPS	"Radiy" (Ukraine)
Rod group and individual control system	RG&ICS	"Impuls" (Ukraine), "Radiy" (Ukraine)
Engineering safety features actuation system	ESFAS	"Radiy" (Ukraine), Impuls (Ukraine)
Steam generator level and feedwater control system	-	Westinghouse Energy Europe
Unit computer information system	CIS	"Impuls" (Ukraine), "Westron" (Ukraine)
In-core reactor monitoring system	IRMS	KhIKA (Ukraine), "SNIIP-Atom" (Russia)
Reactor island normal operation systems	-	"Radiy" (Ukraine), "Impuls" (Ukraine)
Turbine island normal operation systems	-	"Radiy" (Ukraine), "Impuls" (Ukraine)
Refueling machine control system	RMCS	EVIG (Hungary), DIACONT (Russia)
Radiation safety monitoring system	RSMS	"Westron" (Ukraine)

Review of Instrumentation and Control Systems Mission took place at the "Radiy" Corporation site for review of FPGA technology in December 2010.

- The diversity requirement was not implemented in Ukrainian NPP before 2000. Ukrainian regulation, issued in 2000, included this requirement for reactor protection systems as necessary and for other systems of safety class 2 (the highest) as recommended. It would be noted that the diversity requirement caused many contradictions and discussions between the developers of regulations and operators and designers. After discussions, this requirement was included in regulations as obligatory only for protection systems. After a five-year period, specialists began to perceive these requirements as a usual task. The diversity principle has been now incorporated in all reactor protection systems (designer – "Radiy" Corporation).
- Ukrainian companies have elaborated new, their own equipment families (platforms).
- Ukrainian designers have the possibility to use the hardware components from any foreign country. This was impossible before in the USSR, when designers of NPP I&C systems had to use only USSR components.
- An important step was wide use of fiber optic communication lines instead of wire lines.

A set of Ukrainian regulations (NP, 2000; NP, 2003; GND, 2000) were developed to support I&C modernization. These regulations were harmonized as much as possible with requirements of international safety standards and guidelines published before the preparation of these documents. It should be noted that the main principles of IAEA, 2002 were taken in the account in the Ukrainian regulations before the official issue of this document.

All safety important I&C systems designed and produced by Ukrainian companies were brought into compliance with Ukrainian regulations.

The main results of modernizations are the following (Yastrebenetsky, 2004):

- Increase of equipment dependability, availability and reliability;

- Increase of equipment resistance to external impacts;
- Increase of accuracy and time response in the control and checking processes;
- Decrease of time for modernization during unit shutdown for maintenance;
- Improvement of operator information support as well as visualization of technological processes and parameters;
- Improvement of diagnostic functions for I&C systems and technological equipment;
- Decrease of contacts and clip connections by more than 10 times because of high level of integration and fiber-optic lines;
- Compliance with requirements of international safety codes, guides and standards.

OVERALL I&C SYSTEM

Figure 3 shows a general scheme, according to which the overall I&C system of power units with WWER-1000 reactors operated at Ukrainian NPPs.

At a low level, peripheral hardware takes place:

- Sensors (S) of heat engineering, mechanical, electric, neutron-physical values (parameters, describing behaviors of technological processes), external and internal events and states of technological equipment, as well as normalizing transducers and multiplicators of continuous and discrete sensors' signals (not shown in Figure 3).
- Actuators (A), which directly influence on actuator elements of technological equipment - piping valves (flaps, shutters, regulating valves), electric engines, servomotors, etc.

Main control room (MCR) is a center of power unit operational control in operating states, accident control (at least at initial stages) and mitigation of their effects. Systems and equipment of MCR (Figure 4) provide operational personnel with complete, clear, timely and easily visible information and required facilities of manual control, input of commands and guidelines, which allow:

- Monitoring and assessing state and operation of technological systems and equipment, efficiently and safely controlling power unit in all specified operation modes.
- Timely detecting violations of operational limits and normal operation conditions, their causes and taking measures for keeping power unit in a safety state.
- Monitoring and assessing actions of technological and control safety systems in cabinet of violations of operational limits and normal operation conditions and if required – manually prevent these violations.
- Taking required measures for return of a power unit in a safety controlled state after design basis accidents and / or mitigation of effects of severe accidents.

Peripheral equipment of I&C systems is placed at MCR: display and registration equipment (quasi-analog indicators, self-recording instruments, numerical indicators, liquid-crystal and / or plasma board monitors, etc); personnel warning facilities (visual and audio alarms, mnemonic diagrams); manual control elements (keys, keyboard, manipulators, facilities of set-points specification, mode switches, etc.). Here on the basis of peripheral equipment of computer information system are also assembled workstations, from which operational personnel of the power unit (unit shift supervisor, reactor control senior engineer, turbine control senior engineer) perform the following actions:

- Controls technological processes and states of technological systems and equipment.
- Changes power unit operating modes.

Figure 3. Overall I&C system of power units with WWER-1000 reactors after modernization

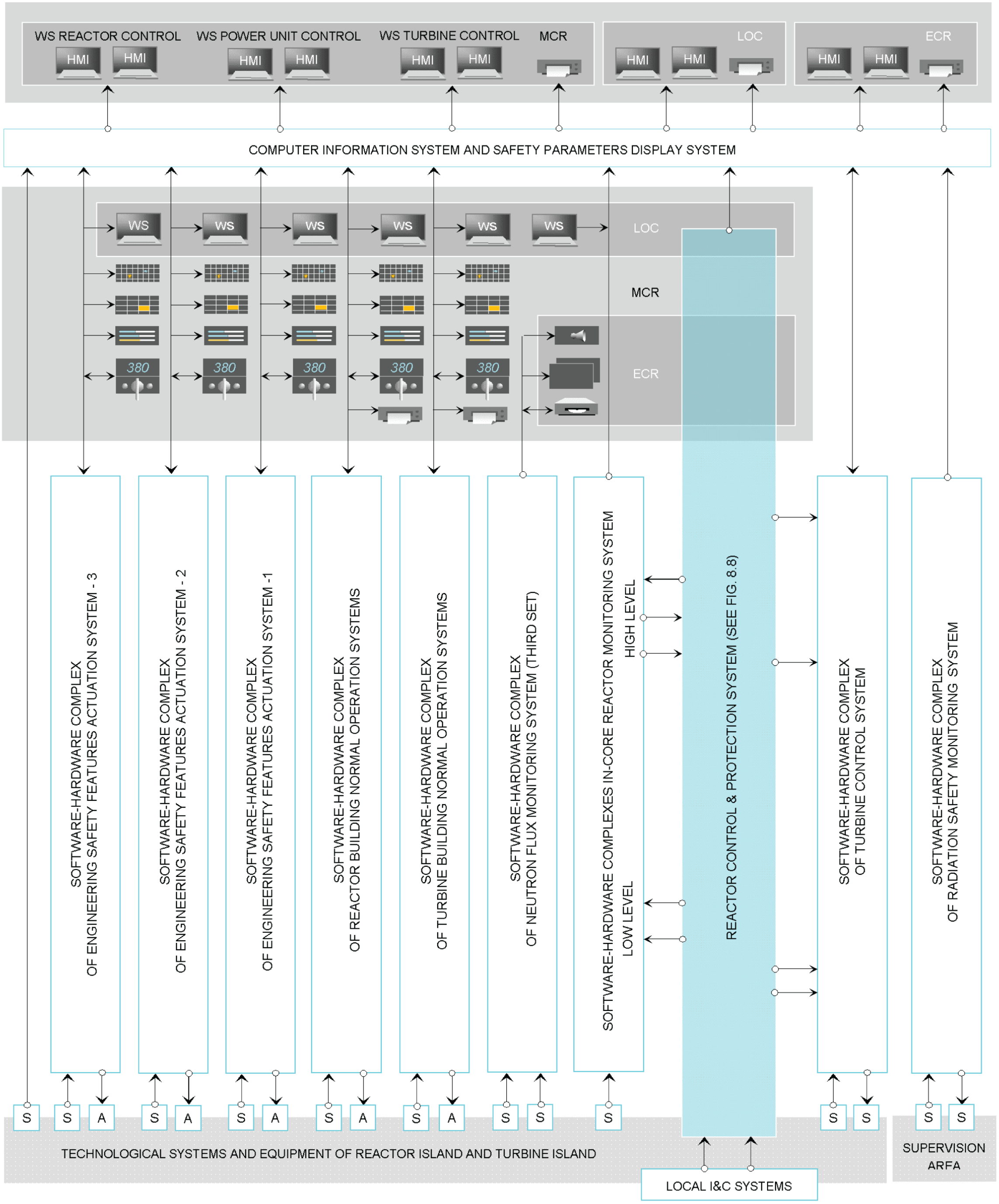
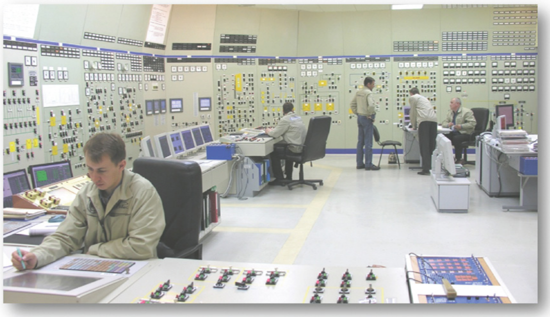

WS REACTOR CONTROL
HMI
HMI
WS POWER UNIT CONTROL
HMI
HMI
WS TURBINE CONTROL
HMI
HMI
MCR
LOC
HMI
HMI
ECR
HMI
HMI
COMPUTER INFORMATION SYSTEM AND SAFETY PARAMETERS DISPLAY SYSTEM
WS
WS
WS
WS
WS
WS
LOC
MCR
380
380
380
380
380
ECR
SOFTWARE-HARDWARE COMPLEX OF ENGINEERING SAFETY FEATURES ACTUATION SYSTEM - 3
SOFTWARE-HARDWARE COMPLEX OF ENGINEERING SAFETY FEATURES ACTUATION SYSTEM - 2
SOFTWARE-HARDWARE COMPLEX OF ENGINEERING SAFETY FEATURES ACTUATION SYSTEM -1
SOFTWARE-HARDWARE COMPLEX OF REACTOR BUILDING NORMAL OPERATION SYSTEMS
SOFTWARE-HARDWARE COMPLEX OF TURBINE BUILDING NORMAL OPERATION SYSTEMS
SOFTWARE-HARDWARE COMPLEX OF NEUTRON FLUX MONITORING SYSTEM (THIRD SET)
SOFTWARE-HARDWARE COMPLEXES IN-CORE REACTOR MONITORING SYSTEM
HIGH LEVEL
LOW LEVEL
REACTOR CONTROL & PROTECTION SYSTEM (SEE FIG. 8.8)
SOFTWARE-HARDWARE COMPLEX OF TURBINE CONTROL SYSTEM
SOFTWARE-HARDWARE COMPLEX OF RADIATION SAFETY MONITORING SYSTEM
S
S
A
S
A
S
A
S
A
S
A
S
S
S
S
S
S
S
TECHNOLOGICAL SYSTEMS AND EQUIPMENT OF REACTOR ISLAND AND TURBINE ISLAND
LOCAL I&C SYSTEMS
SUPERVISION ARFA

Figure 4. Main control room at Rovno NPP



- Monitors actions of normal operation control systems and safety systems.
- If required, inputs guidelines for control I&C systems dedicated to elimination of detected deviations.
- Issues commands of remote control and monitors their performance by technological equipment.

Emergency control room (ECR) is a specifically equipped room, territorially separated and completely independent from MCR, having nuclear electric communications and own facilities of habitability and operability (continuous presence of personnel is not provided). Systems and equipment of ECR provide personnel with a possibility to control significant process parameters, assess power unit state and issue commands to technological systems and equipment, required for transfer of the reactor to sub-critical state, keep it in this state for a sufficiently long time and control residual heat removal in situations when the possibility to perform these functions from MCR is lost, including failures of control I&C systems, initiating safety shutdown and cooling of reactor. Information on the neutron flux density required for control is displayed in video monitors placed in ECR, included into the structure of software-hardware complex of neutron flux monitoring system (third set). Peripheral equipment of adjacent I&C systems is also placed at ECR: quasi-analog indicators, numerical indicators, visual and audio alarms, mnemonic diagrams, manual control elements (see Figure 3).

NPP control room obtains from I&C systems of all NPP power units information on their state and operation, required for a shift engineer to control and coordinate operation of common systems.

The central part of overall I&C systems is formed by relatively isolated individual I&C systems, interacting during execution of informational and control functions.

Unit computer information system (CIS) performs:

- Collection and generation of signals from sensors of heat engineering, electric and other parameters, from other informational and control power unit systems and also from Radiation safety monitoring (RSM) system.
- Informational support of operational personnel during making decisions for control of technological processes and equipment of the power unit (control of deviations and technological parameters from specified values, deviation alarm, calculation and analysis of technical and economic indicators, etc.)
- Archiving (memorization and storage) of parameter values, events, states, actuation of protection and interlocking, actions of operational personnel.
- Display on video monitors and registration of current information and archival data during by personnel guidelines during normal operation, in emergencies and accidents (for control of accidents and further analysis and assessment of occurrence causes, ways of behavior and accident effects).

Safety parameters display system (SPDS) provides informational support to the operator in quickly determining deviations in unit operation.

In this cabinet, the SPDS can be used to analyze and diagnose causes of the onset of disturbances in unit operation and to identify corrective actions. Description of SPDS will be given in Chapter 11.

In-core reactor monitoring system (IRMS) monitors neutron and thermo-hydraulic parameters of the reactor core and the primary circuit; controls distribution of neutron flux density across the section and along the height of the core and predicts their changes; generates signals, which warn operational personnel about violations of specified operational limits and initiate actuation of preventive protection of the reactor facility in case of such violations; archives and displays monitoring results.

In IRMS two hierarchical levels are provided. The lower level contains sensors of pressure, flow rate, temperature, measuring channels of the neutron flux density located inside the reactor and means of collection, transformation of sensors signals and preliminary data processing; the upper hierarchical level is formed by dual-computer system. Information required for calculations is input in IRMS from adjacent I&C systems, included in the the reactor control and protection system (shown in Figure 7): information on the neutron flux density (reactor neutron power) – in the form of continuous signals from second and third set Neutron flux monitoring system (NFMS), information on the position of control rods – in the form of continuous signals from Rod group and individual control system (RG&ICS), information on preliminary protection – in the form of discrete signals from the emergency and preventive reactor protection system (E&PRPS). In turn, IRMS outputs discrete signals of violations of specified operational limits for local energy release, departure from nucleate boiling on the surface of fuel elements and coolant temperature at the output of fuel assemblies in E&PRPS.

Engineered safety features actuation systems (ESFAS) are intended to initiate actions of technological systems and power unit equipment, ensure their monitoring and control during execution of specified functions in any operation modes on the reactor facility (including design basis and beyond design basis accidents). Systems of planned and emergency cooling, emergency supply of feedwater into steam generators, make-up-blowdown of the primary circuit, drain water collection, sprinkling system, etc. relate to such technological systems.

In the overall I&C system of power unit with WWER-1000 reactor, three ESFAS are provided, where functions of technological protection, being the most important for safety, are executed independently in each of such a system and less important are distributed among them.

Each ESFAS contains:

- Technological parameter sensors and normalizing transducers.
- Three independent channels, in each of them monitoring of controlled parameters is performed and technological protection and interlocking signals are generated.
- Means of automatic water level control in steam generators, discharge pressure of an emergency feedwater pump, pressure in a fast acting steam dump system, etc.
- Devices of remote control of actuators and technological equipment of the power unit.
- Keys of mode selection and specification of remote control commands, set in MCR and ECR.

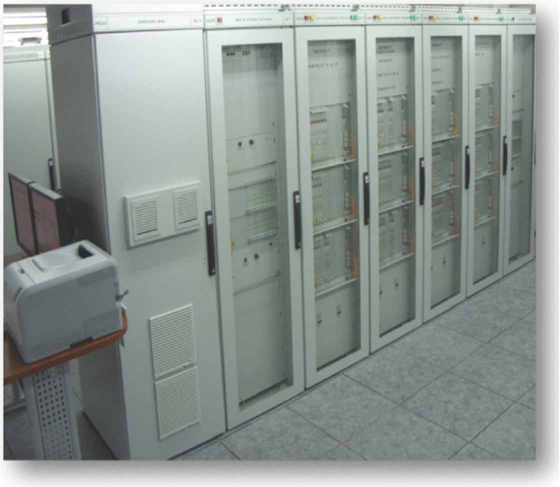
According to the initial design, ESFASs were assembled on the basis of a specifically developed equipment family – a universal hardware complex, in which computers were not used: all safety important control functions were implemented by hardware and informational ones, connected with technological protection, interlocking and remote control, were transferred for execution in CIS. In the process of modernization, earlier used equipment is substituted by software-hardware complexes (SHC ESFAS), implemented on the basis of RADIY PLATFORM or MSKU (see

Chapter 1 and Figure 5), which besides control functions also execute informational functions of monitoring, display, alarm, archiving and registration independently from CIS.

Reactor island normal operation systems and turbine island normal operation systems support specified values of power unit technological parameters. Pressure in the primary circuit, pressure drops on main circulation pumps sealed, pressures and levels in make-up-blowdown deaerators and boron regulation, the coolant level in the pressurizer, temperature difference of the primary circuit and pressurizer in a planned heating and cooling mode, etc. are regulated in the reactor island. Main and start-up level regulators in steam generators, steam pressure regulators in deaerators, level regulators in the turbine condenser, in reheaters of low and high pressure, productivity of turbine feedwater pumps, etc. are provided in the turbine island.

According to the design, automatic regulators were implemented on the basis of general industrial equipment families, which besides nuclear power engineering were also used at thermal power stations, in chemistry, metallurgy and other industry branches. In the process of modernization, these regulators were changed by software-hardware complexes, implemented on the basis of RADIY PLATFORM or MSKU.

Figure 5. Part of software-hardware complex of engineered safety features actuation system on the base of RADIY PLATFORM



Additionally to regulation of technological parameters, SHC normal operation systems perform:

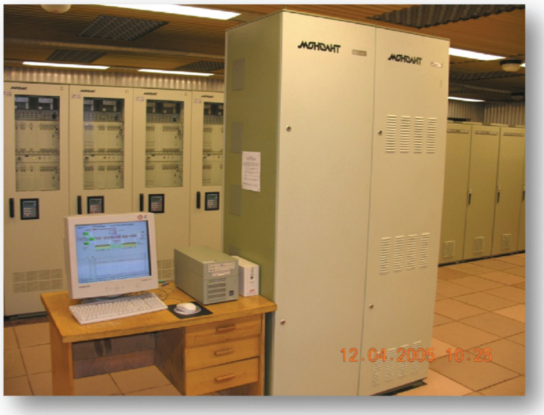
- Power supply to sensors, reception and primary processing of signals from sensors.
- Remote control of technological equipment.
- Interlocking of regulators and control valves.
- Archiving, display, preparation and transmission of information about technological parameters, state of sensors and actuators, interlocking actuation, etc. into CIS.

In 1986 application of the first microprocessor regulating systems (automatic turbine control systems ASUT-1000-2) was started at Ukrainian NPPs. The system performed monitoring and automatic digital control during start-up, functioning in operating modes and shutdown of a turbine, also providing operational personnel with a possibility of a remote turbine control from MCR. In the modernization process, this system was substituted by a new software-hardware complex of turbine control system (Figure 6) on a set of power units.

At South-Ukrainian NPP, feedwater level control systems in steam generators, implemented according to the design on the basis of general industrial equipment family, were substituted during modernization by a new steam generator level and feedwater control system (developer and manufacturer – Westinghouse Energy Europe in partnership with “Westron” Corporation).

Besides systems shown in Figure 3, the overall unit I&C system of the power unit with WWER-1000 reactor also contains other safety related I&C systems, including:

Figure 6. Software-hardware complex of turbine control system



- Refueling machine control system, implemented by EVIG (Hungary) on power units of South-Ukrainian NPP, and DIACONT (Russia) on power units of Rovno NPP.
- Radiation safety monitoring system (RSMS), developed by "Westron" and implemented on all Ukrainian NPPs that performs: continuous radiation monitoring of gamma background levels, activity of inert gases, beta-sprays and iodine in NPP rooms; continuous technological control of the primary and secondary coolant activity, technical water in special water and gas purification systems; continuous radiation control of NPP influence on the environment (control of activity of tail water and gas-aerosol emission into a ventilation tube).
- Automatic control system of standby diesel generator-stations with one or two diesel-generators, supplying safety systems and / or common plant systems in case of power unit de-energizing in accidents (developer and manufacturer – "Westron," implemented on power units of South-Ukrainian NPP and Rovno NPP). The system provides: availability of a standby diesel-generator station for start-up and rapid load acceptance; manual and automatic start-up control; synchronization of shaft generator speed with a network power frequency; automatic support of power operation during a long time period; automatic emergency shutdown by actuation of technological protection (with a blocking of the next start-up); standard shutdown, including performance of final operations.

A relatively isolated part of the overall I&C system, providing control of the chain reaction of nuclear fuel fission, will be considered in more detail further. It contains the most closely interrelated individual I&C systems, which are called the reactor control and protection system in Ukraine and Russia.

REACTOR CONTROL AND PROTECTION SYSTEM

The reactor control and protection system (RC&PS) is intended for: measurement of neutron flux density and its rate of change; monitoring of technological parameters and reactor facility power in manual and automatic mode; emergency and preventive reactor protection. Emergency protection, having a priority over all other control functions, provides rapid transfer and long-term support of the reactor core in sub-critical state, preventive protection – limitation or decrease of reactor power to a safe level.

The fundamental "virtuality" of the RC&PS system, which thus does not have required attributes of any real system such as individual terms of reference for development, design and operational documentation, data base, etc. should be mentioned. In international standards there is no analogue to the notion RC&PS, though in Russia and Ukraine this term is widely used, in particular, in the organizational structure of NPP, technological regulations, operation instructions, etc. However, it should be kept in mind that this term relates not to one system, but to several interacting I&C systems, which together perform all functions provided for RC&PS. Just in this sense, the concept, the term that represents it and abbreviation are used in this book.

RC&PS (Figure 7) consists of individual I&C systems:

- Neutron flux monitoring system (second and third sets).
- Emergency and preventive reactor protection system (first and second sets).
- Reactor power control, unloading, limitation and accelerated preventive protection system.
- Rod group and individual control system.

Real I&C systems, united by the concept RC&PS, were developed by different organizations and / or on the basis of different equipment families and modernized in different time, so each of them can be considered individually.

Neutron Flux Monitoring

The main purposes of the neutron flux monitoring system (NFMS) are: monitoring of reactor relative neutron power and rate (period) of its change; generation of discrete signals by specified conditions, which initiate actuation of the emergency protection (rapid suppression of chain reaction in the reactor), and preventive protection (decrease of reactor power or prohibition on power increase); generation analog signals, by which the current value of relative neutron power (one of the main regulated reactor facility parameters) is determined.

In addition, NFMS performs:

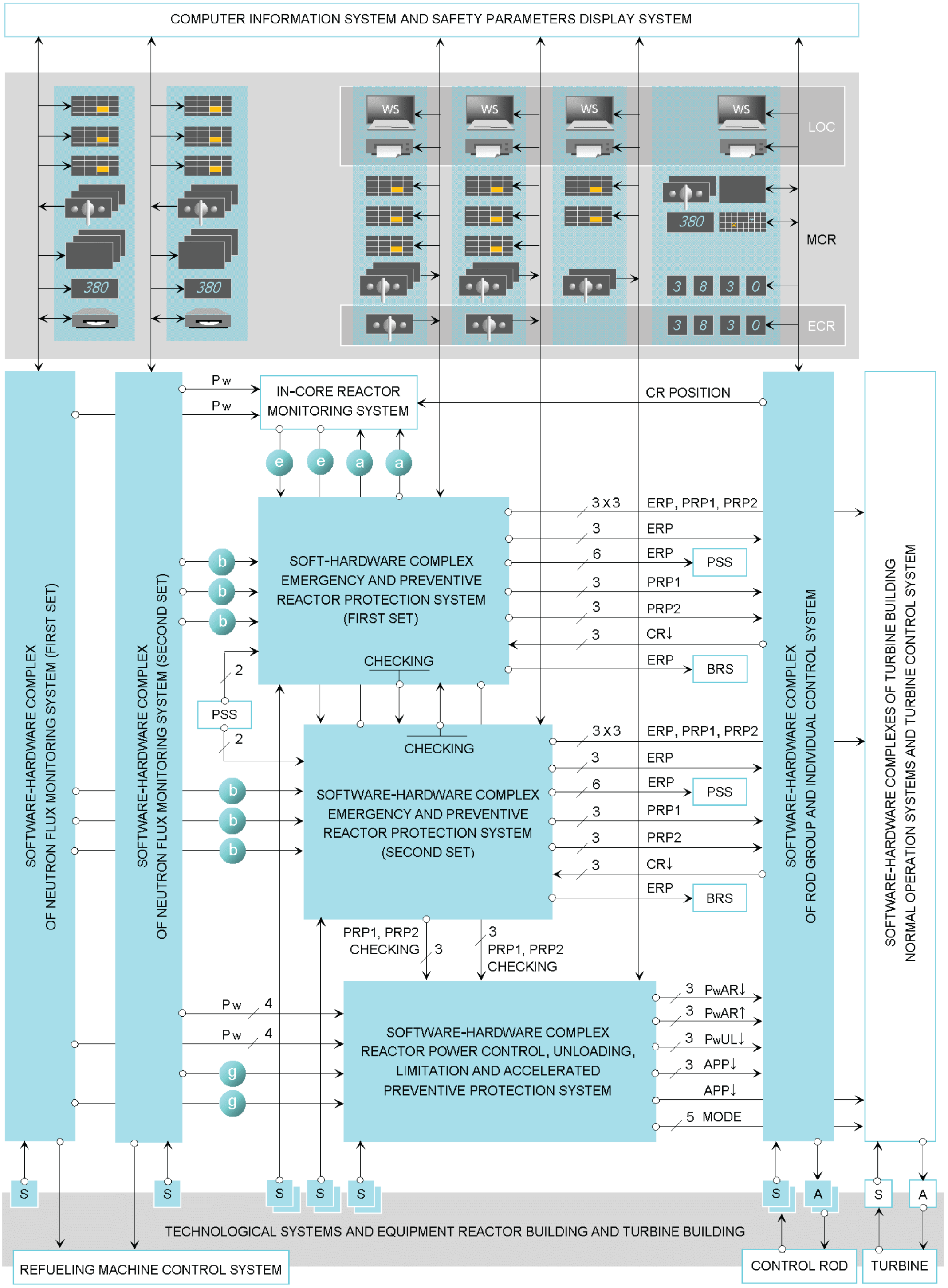
- Calculation and display of reactivity.
- Display of current values of neutron power and a period of its change.
- Warning of personnel about violations of operational limits (normal and safe operation) by neutron power and a period of change.
- Monitoring of the system technical state and diagnostics of failures of the system and its components.
- Archiving of current values of reactivity, neutron power, period of its change and display of archival information.
- Formation and output of messages about values of monitored parameters and the current system technical state for transmission in IRMS and CIS through a local network.

NFMS performs its functions in all reactor operation modes: sub-critical, transient, stationary, emergency, including maximum design basis accident and also during nuclear fuel reloading. Significant peculiarity of NFMS is a wide range of neutron flux density measurement, corresponding to a change of relative neutron power from 10$^{\%\%}$ to 120% of nominal.

The RC&PS includes two independent NFMS (first and second sets in Figure 7), operating simultaneously and being interredundant. Each NFMS monitors neuron flux during nuclear fuel reloading, reactor start-up and power operation. One more NFMS (third set in Figure 3), providing a possibility to monitor and control the reactor from ECR, is not contained in RC&PS.

The basis of each NFMS is formed by a software-hardware complex, together with it peripheral equipment is supplied: sensors S (neutron flux detection devices); warning means (visual alarms); manual control means (set-points device, mode switches); devices of archiving and displaying of values, of relative neutron power, period, reactivity and set-points (built-in panel computers, recordings on removable media device); device of digital indication of neutron power and period (digital indicator).

Figure 7. Reactor control and protection system after modernization


COMPUTER INFORMATION SYSTEM AND SAFETY PARAMETERS DISPLAY SYSTEM
WS
WS
WS
WS
LOC
380
380
380
MCR
3 8 3 0
3 8 3 0
ECR
SOFTWARE-HARDWARE COMPLEX
OF NEUTRON FLUX MONITORING SYSTEM (FIRST SET)
SOFTWARE-HARDWARE COMPLEX
OF NEUTRON FLUX MONITORING SYSTEM (SECOND SET)
Pw
Pw
IN-CORE REACTOR
MONITORING SYSTEM
CR POSITION
e
e
a
a
b
b
b
2
PSS
2
SOFT-HARDWARE COMPLEX
EMERGENCY AND PREVENTIVE
REACTOR PROTECTION SYSTEM
(FIRST SET)
CHECKING
3x3
ERP, PRP1, PRP2
3
ERP
6
ERP
PSS
3
PRP1
3
PRP2
3
CR↓
ERP
BRS
CHECKING
SOFTWARE-HARDWARE COMPLEX
EMERGENCY AND PREVENTIVE
REACTOR PROTECTION SYSTEM
(SECOND SET)
b
b
b
3x3
ERP, PRP1, PRP2
3
ERP
6
ERP
PSS
3
PRP1
3
PRP2
3
CR↓
ERP
BRS
SOFTWARE-HARDWARE COMPLEX
OF ROD GROUP AND INDIVIDUAL CONTROL SYSTEM
SOFTWARE-HARDWARE COMPLEXES OF TURBINE BUILDING
NORMAL OPERATION SYSTEMS AND TURBINE CONTROL SYSTEM
PRP1, PRP2
CHECKING
3
3
PRP1, PRP2
CHECKING
Pw
4
Pw
4
g
g
SOFTWARE-HARDWARE COMPLEX
REACTOR POWER CONTROL, UNLOADING,
LIMITATION AND ACCELERATED
PREVENTIVE PROTECTION SYSTEM
3 PwAR↓
3 PwAR↑
3 PwUL↓
3 APP↓
APP↓
5 MODE
S
S
S
S
S
S
A
S
A
TECHNOLOGICAL SYSTEMS AND EQUIPMENT REACTOR BUILDING AND TURBINE BUILDING
REFUELING MACHINE CONTROL SYSTEM
CONTROL ROD
TURBINE

In each NFM three independent interredundant channels can be selected (Figure 8).

Channel includes:

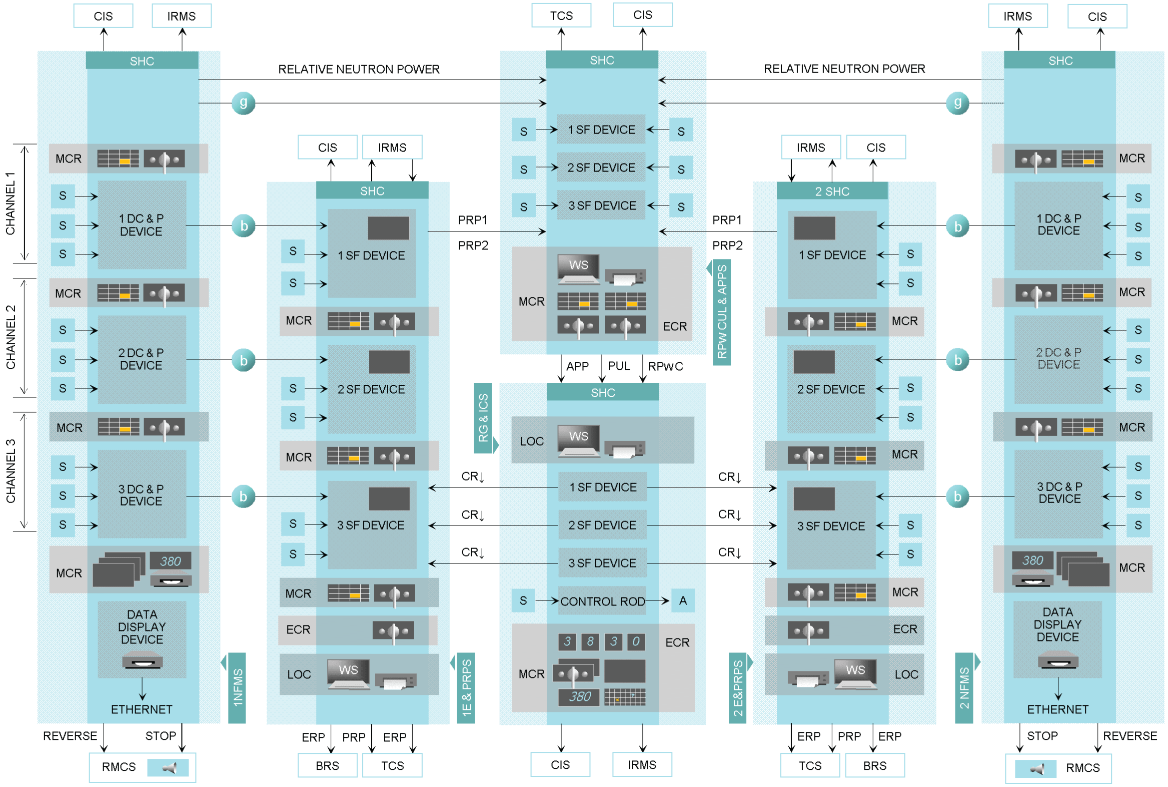
- Three neutron level detectors (sensors S) – for measurement of neutron flux density in subranges controlled during nuclear fuel reloading, reactor start-up and power operation, respectively.
- Devices for data collection and processing (DC&P 1, 2 or 3), implemented in a separate cabinet.
- Manual control means and warning means located in MCR.
- Device (not shown in Figure 8) that during nuclear fuel reloading provides a possibility for manual control of transfer mechanisms of neutron level detectors and indication of their position.

Built-in panel computers, recordings on removable media device, digital indicator located in MCR, and audio alarm placed on the board of refueling machine control system (RMCS) are common for the three channels.

Each device for data collection and processing:

- Receives encoded signals, corresponding to neutron flux density value, from neutron level detectors, operating in a required measuring subrange.
- Calculates relative neutron power Pw (in percentage of the reactor power nominal value), the period of power change T and reactivity.
- Compares calculated values of relative neutron power and the period with specified limit values (set-points).

Figure 8. Structure of a typical reactor control and protection system



Emergency protection set-points are assigned by power (ERP “Pw”) and period (ERP “T”) and preventive protection set-points by power (PRP1 “Pw,” PRP2 “Pw”) and period (PRP1 “T,” PRP2 “T”), separately for monitoring during reloading, startup, and operational subrange, and also upper limit of reactor power automatic regulation (ULAR “Pw”), that corresponds to 102% of reactor relative neutron power.

If relative neutron power or a period exceed specified for them limit values (i.e. during fulfillment of any of conditions Pw ≥ ERP “Pw,” T ≤ ERP “T,” Pw ≥ PRP1 “Pw,” T ≤ PRP1 “T,” Pw ≥ PRP2 “Pw,” T ≤ PRP2 “T”), relevant output of devices for data collection and processing (channel output) generates discrete signals, transmitted to inputs of emergency and preventive reactor protection system (E&PRPS). Analog signals, defining the value of relative neutron power Pw, are transmitted from inputs of each channel of the first and second NFMS to inputs of reactor power control, unloading, limitation and accelerated preventive protection system (RPW CUL & APPS).

In the same system, discrete signals generated in channels 1 NFMS and 2 NFMS are transferred when relative neutron power exceeds 25% and 75% of the nominal value (Pw ≥ 25%; Pw ≥ 75%) and when reactor relative neutron power achieves the upper limit of reactor power automatic regulation (Pw ≥ ULAR “Pw”).

In NFMS output signals are also generated:

- For IRMS and CIS - analog signals, representing specified (limit) and current (averaged by three channels) values of relative power and a period, and discrete signals, defining a measuring at the moment neutron flux subrange (corresponding to nuclear fuel reloading, reactor start and power operation) and a result of checking (diagnostic) of NFMS.
- For RMCS – discrete signals, warning of exceeding values of relative power or period specified as set-points of preventive or emergency protection for a nuclear fuel: STOP (if Pw ≥ PRP1 “Pw” or T ≤ PRP1 “T”) and REVERS (if P ≥ ERP “P” or T ≤ ERP “T”).

Current values of relative power and period calculated in each channel and also averaged among three channels are displayed on digital indicators and built-in panel computer screen (in the form of digitized diagrams and histograms). Besides them, lower and upper limits of neutron power in each subrange are displayed on built-in panel computers screen, a current subrange is initiated, signals on achievement of each of the specified set-points of power and period are generated.

The data display device receives information from DC&P 1, 2 and 3, saves it in an archive (in a hard disk), creates (edits) archival file footages, and provides their review and duplication on external media. Possibility of data output in Ethernet network for transmission of digital messages in IRMS and CIS is provided.

Emergency and Preventive Protection

Functions of emergency and preventive protection are performed by two independent emergency and preventive reactor protection systems (E&PRPS). Each system contains:

- Software-hardware complex (SHC).
- Sensors of temperature, pressure, level, pressure drop, frequency, electric power, technological equipment state.
- Peripheral devices (placed in MRC): warning means (visual alarms) for the reflection of the SHC state (faults, disconnections)

and indicating a cause, what initiated the emergency or the preventive protection; manual control means (keys for initiation of commands of emergency or preventive protection and confirmation of messages).

- Key (placed in ERC) for manual initiation of emergency protection commands.
- Cables for connections.

E&PRPS has three independent interredundant channels. Each channel has a full set of required sensors, independent from sensors of other channels, and performs all main functions of emergency and preventive protection. The central part of each channel - signal forming (SF) device - implemented in a separate cabinet and supplied by built-in panel computer for set-points input and adjustment.

The following is common for three SF devices (channels): cross output cabinet (not shown in Figure 8); elements (keys) of manual control and visual alarms, placed in MCR and ECR; workstation (WS) of data archiving and display, and laser printer, located in a room of a shift personnel that monitors a state and provides maintenance and recover of reactor control and protection system (LOC); automated work places of technologist and operator (not shown in Figure 7 and 8).

Each channel receives:

- Analog and discrete signals from sensors S of this channel.
- Discrete signals Pw ≥ ERP “Pw,” T ≤ ERP “T,” Pw ≥ PRP1 “Pw,” T ≤ PRP1 “T,” Pw ≥ PRP2 “Pw,” T ≤ PRP2 “T” from a proper channel 1 NFMS (2 NFMS).
- Discrete signals from IRMS (violations of specified operational limits of local energy release, departure from nucleate boiling on the surface of fuel elements and coolant temperature at the output of fuel assemblies).
- Discrete signals from a electric supply system (lack of supply voltage on feeders).
- Commands from control keys in MCR and ECR.

In addition, at the input of each SHC channel, a discrete signal is supplied during deactivation of another SHC, for example, for checking or maintenance.

The channel that has detected a deviation of at least one monitored (measured or calculated) parameter over the set-point limit of emergency protection actuation, or identified a failure of any of specified safe operation conditions, or received from proper channel 1 NFMS (2 NFMS) a signal Pw ≥ ERP”Pw,” T ≤ ERP”T” or an operator’s command (from a key “ERP,” placed in MCR or ECR), forms a discrete signal that is transmitted to the cross output cabinet. On the basis of these signals, obtained from, at least, two or three channels, cross output cabinet generates (according to an accepted logical condition “two-out-of-three”) and outputs an emergency protection command (ERP).

- **At the output of three channels of the actuation system (RG&ICS):** Initiates reactor emergency shutdown due to the main and standby power from all control rods, causing their drop in the reactor core.
- **At the first and second output of a power supply system of control rod drives:** Initiates emergency shutdown due to deenergization of alternate current on both inputs of power supply to all control rods.
- **At the outputs of three channels of a turbine control system (TCS):** Initiates actions, leading to turbine unloading in case of reactor emergency shutdown.
- **At the input of the boron regulation system (BRS):** Initiates connection of high-pressure boron injection pump.

At the same time, at one of outputs of the cross output cabinet a signal, indicating the cause of emergency reactor protection actuation (switches a proper board in MCR) is generated. Command of ERP and a signal, indicating the actuation cause, are stored at the cross cabinet output until an operator dumps them, using proper keys in MCR.

In the same way, the cross output cabinet forms and outputs a preventive protection command (PRP1 or PRP2) on the basis of signals, received at least from two or all three channels, which have detected deviations of any controlled parameter over the set-point limit of actuation PRP1 or PRP2, or identified violations of relevant normal operation conditions, or received a signal Pw ≥ PRP1 ”Pw,” T ≤ PRP1 ”T” or Pw ≥ PRP2 ”Pw,” T ≤ PRP2 ”T” from 1 NFMS (2 NFMS) or an operator’s command from a key “PRP1” in MCR.

Command PRP1 is supplied:

- **To inputs of three channels RG&ICS:** Initiates decrease of reactor power due to sequential drop of groups of control rods into the core.
- **To inputs of three channels of TCS:** Initiates actions, leading to a decrease of turbine power.
- **To outputs of three channels of reactor power control, unloading, limitation and accelerated preventive protection system (RPw CUL & APPS):** Prohibits operation of the automatic regulator that could prevent power decrease.

Command PRP2, supplied from the cross output cabinet to similar inputs of the same systems, prohibits any actions which could cause power increase of the reactor or turbine.

Simultaneously with delivery of a command PRP1 or PRP2 at the output of the cross output cabinet, a signal is generated to indicate the reason of actuation that switches a proper board in MCR. Commands PRP1 and PRP2 are output till there are violation, which caused them; a signal of actuation cause is stopped by a key from MCR.

Similar signals and commands are generated at outputs of another SHC. All mentioned actions of adjacent systems may be initiated by commands of each of both SHC. Digital messages, containing current information, are transmitted from both SHC to the unit computer information system.

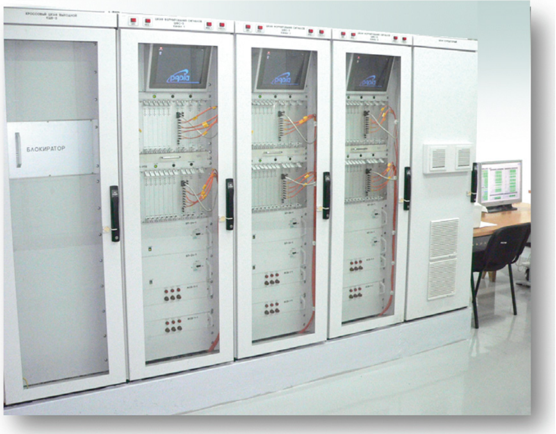
A detailed description of E&PRPS will be given in Chapter 9.

Automatic Regulation, Unloading, Power Limitation

Functions of reactor power control, unloading, limitation and accelerated preventive protection (unit accelerated unloading) are performed by RPw CUL & APPS that contains sensors S of heat engineering parameters, events, states and a software-hardware complex, implemented on the basis of RADIY PLATFORM (Figure 9), with devices of alarm and control and a workstation (WS), located in MCR.

The system (see Figure 8) has three independent interredundant channels, according to the “two-out-of-three” logic. Each channel has a full

Figure 9. Software-hardware complex of reactor power control, unloading, limitation and accelerated preventive protection system



set of required sensors, independent from sensors of other channels. The central part of each channel - signal forming (SF) device - implemented in a separate cabinet, in which two plug-in card cage (crates) with mounted in them in-coming modules (cards) are placed, is provided. One of crates performs functions of automatic power control, another one controls unloading, power limitation and initiates accelerated preventive protection of the reactor. Each cabinet supplied by built-in panel computers for set-points input and adjustments.

The following is common for three SF devices (channels):

- Cross output cabinet (not shown in Figure 8).
- Workstation (WS) of data archiving and display, and laser printer.
- Visual alarms for the reflection of the SHC state and indicating the cause that initiated unloading of reactor power.
- Keys for the task of the control (regulation) modes, initiation of commands for unloading and accelerated preventive protection and confirmation of messages by MRC personnel.
- Automated work places of technologist and operator (not shown in Figure 7 and 8).

Crate performing the reactor automatic power regulation function receives:

- Analog signals from pressure sensors above the core and main steam collector.
- Analog signals from 1 NFMS and 2 NFMS, representing a value of relative neutron power Pw, and discrete signals Pw ≥ 25%, Pw ≥ 75%, Pw ≥ «Pw», Pw ≥ ULAR “Pw.”
- Commands PRP1 (regulation prohibition), PRP2 (power increase prohibition) from 1 E&PRPS and 2 E&PRPS, and discrete signals CHECKING of proper system deactivation (shown in Figure 7).
- Discrete signals, defining a selected operation mode (automatic and remote) and control mode from an alarm and control board, placed in MCR.

Discrete output signals RPwC, generated in case of a regulated parameter deviation (relative power or pressure in main steam collector) from the specified value, initiate actions of the actuation system RG&ICS that minimizes this deviation due to lifting or dropping of a working (regulating) group of control rods into the reactor core. In TCS from cross cabinet signals, defining selected control mode RPwC are transmitted. Similar information of each channel and output regulation commands, actions caused by them, prohibition of decrease and (or) increase of power, state (operability) of each channel are initiated on the indication and control board. General signals of operability failure and / or deactivation of any of channel control board switching in MCR.

Crate performing functions of power unloading and limitation (PUL) and accelerated preventive protection (APP) receives:

- Analog signals from sensors and normalizing transducers of coolant temperature, pressure, power frequency and power of main circulation pumps.
- Discrete signals from sensors of turbogenerator state (disconnection, setting of stop valves, generator unloading).
- Analog signals, representing relative neutron power value and discrete signals Pw ≥ 25% and Pw ≥ 75% from 1 NFMS and 2 NFMS.
- Discrete signals CHECKING of deactivation of 1 E&PRPS (2 E&PRPS).
- Commands from keys “PUL” and “APP,” placed in MCR.

On the basis of signals received from two or three channels, in which specified power unloading conditions were detected, the cross cabinet generates and delivers to input of three channels of the actuation system RG&ICS a command PUL. This command causes reactor power decrease due to a sequential drop of groups of control rods in the reactor core with a nominal speed. Information about output of a command PUL and state (availability or inoperability) of each channel is indicated on an alarm board, placed in MCR. Common signals of violation of operability and / or deactivation of any channel, actuation of power unloading function and equipment state, caused unloading and of access in any cabinet control switching of a proper board in MCR.

In case of disconnection of the main equipment, setting of turbine stop valves, disconnection of the unit from electrical power system, when unit power exceeds 75% of the nominal value, or direct input of a command with a key located in MCR, the cross output cabinet forms (on the basis of signals received from two or three channels) and outputs a command of accelerated preventive protection (APP):

- At inputs of three channels of the actuation system RG&ICS (initiates rapid reactor power decrease due to deenergization of the main and standby power supply to all control rods of a preliminary specified group and their drop into the core).
- At inputs of TCS (initiates actions causing proper turbine power decrease).

Simultaneously at outputs of the cross cabinet, signals form for switching the board in MCR, initiating actuation of APP and the cause of actuation, are generated. Command APP and the cause signal are stored at the output of the cross cabinet until they will be reset by the operator with proper keys in MCR. Current, diagnostic and archival information is received by the workstation and transmitted in CIS of the power unit.

Rod Group and Individual Control

Rod group and individual control is performed in all modes of power unit operation and also during scheduled and emergency shutdowns and influences the process of chain reaction in the core for keeping the reactor power and / or other parameters of reactor facility within specified limits, for power change or transfer of the reactor to a subcritical state. Specified functions are performed by the rod group and individual control system (RG&ICS).

During power unit operation, simultaneous change in the state of several (group) control rods (group control) or one (any) selected control rod (individual control) is executed in the core. In case of scheduled reactor shutdown, performed for equipment maintenance or nuclear fuel reloading, all groups of control rods are sequentially inserted in the core by an operator command that terminates the chain reaction. Emergency shutdown by a command ERP, received from the emergency reactor protection system, is executed by disconnection of alternating current at inputs of power electrical supply, from which control rods are fed, and deenergization of main and standby power from their drives. This causes control rods' drop in the core under gravity that suppress the chain reaction (reactor shutdown).

RG&ICS provides group and individual control of control rods in automatic and manual mode. Automatic group control is performed by commands of the emergency reactor protection (ERP), preventive reactor protection (PRP1), accelerated preventive protection (APP), power unloading and limitation (PUL) and reactor power control (RPwC).

By operator's commands manual (remote) group and individual control is performed:

- Lifting and dropping with a working speed of any group of control rods or transfer of groups one after another in a project sequence.

- Lifting and dropping with a working speed of any (one) control rod.
- Lifting and dropping with a working speed of one (fifth) group of control rods.

RG&ICS contains: sensors (S) of control rod position; step electromagnetic control rod drivers (A); software-hardware complex (SHC) with a workstation WS and printer, placed in LOC; device for selection, control and monitoring of selected CR and selected group of CR (switches, digital indication devices, mnemonic diagram with built-in keys and panel computer), placed in MCR; digital indication devices of all control rods positions, placed in MCR and ECR.

Functions of group and individual control command formation are performed by three independent interredundant channels. The central part of each channel - signal forming (SF) device, implemented in a separate cabinet.

Each channel receives:

- Commands of emergency reactor protection (ERP) and preventive reactor protection (PRP1, PRP2) from proper channels 1 ERPS and 2 ERPS.
- Commands of power unloading and limitation (PUL), accelerated preventive protection (APP) and reactor power control (RPwC) from proper channels RPwCUL&APPS.
- Group number CR, selected for manual control, and commands of lifting or dropping of a selected group.
- Coordinates of CR, selected for manual control, and commands of lifting and dropping of a selected CR.
- Information on position of all CRs by core height, deenergization of electromagnets (drop of CR) and duration of dropping in the form of digital messages from position control cabinets CR.
- To cabinets of control rod drives (not shown in Figure 8) – control signals, initiating power supply dump from all drives (by command ERP) or from preliminary selected group of rods (by command APP).
- To cabinets of control rod drives – signals, which control transfer of a group of CRs or an individual CR in manual mode (by a command from a monitoring and control board) or in an automatic mode (by commands PRP1, PUL, APP, RPwC).
- To a monitoring and control board – information on the position of all CRs by height and mismatch of CR in each group and an alarm message in case of exceeding an allowable mismatch of at least of one group.

Direct control of position of each CR is executed individually by independent channels in cabinets of control rod drives. Each channel:

- Receives control signals from cabinets 1SF, 2SF, 3SF initiated by commands ERP and APP, and deenergizes electromagnets of control rod drive after receiving signals from, at least, of two cabinets.
- Receives digital messages from cabinets 1SF, 2SF, 3SF, processes received information according to a logical condition “two-out-of-three,” generates and outputs a sequence of impulses to CR, causing its lifting or dropping (or keeps CR still in case of lack of commands for transfer of this CR in message, received from, at least, two SF).
- Stops outputting a sequence of impulses after a controlled CR reaches the limit position (upper or lower).
- Automatically switches the control rod drive to supply from a standby source in case of disappearance of the main power source or failures in control circuits.

During a command activity PRP2, received from 1 ERPS or 2 ERPS, output of signals for upward transfer of CR is blocked.

Indication elements and panel computer monitor, built in the monitoring and control board, provide the following information: the number of a controlled group CR; coordinates of CR selected for individual control; direction of transfer; position of CR by height and other information on operator's request.

Inbuilt diagnostics facilities perform:

- Continuous automatic monitoring of the technical state of all components of SHC RG&IC, adjacent peripheral equipment and communication lines of signals and messages.
- Processing of received information, archiving, display (continuous and on an operator's request) of current and archival information, output of diagnostic messages to CIS and IRMS.
- Audible warning in case of detection of operability failures, output of proper warning messages on a video monitor screen, generation and output of generalized signals of unavailability to CIS, IRMS and a board to MCR.
- Detail description of rod group and individual control system is given in Chapter 10.

Solutions and Recommendations

Overall instrumentation and control system described in this chapter is the result of modernization of individual I&C systems. These systems were implemented at Ukrainian NPPs according type design for WWER-1000 units, what were elaborated in USSR in 70-th.

Computer technique in this time was on initial stage of implementation at NPPs because low reliability, absence of personnel who can operate with new technique. Common structure of overall instrumentation and control system is characteristic for stage of automatic that preceded of computers appearance. Step by step modernization of individual I&C systems can realized only in frame of this structure. The same is related to equipment of main and emergency control rooms.

Overall instrumentation and control system can be considerably changed only in connection with building of new power units (for Ukraine – Khmelnitsky NPP units 3 and 4). Design of overall instrumentation and control system for new units can based on other principles, used of all advantages of modern information technology, local nets, new element base, etc. Some recommendation for design of overall instrumentation and control system for new units: save division on such components as individual instrumentation and control systems; expand types of functions (fire signalization, fire fighting, post accident monitoring, etc); improve connections between components; unify technical decisions, including platforms.

FUTURE RESEARCH DIRECTIONS

The Fukushima-1 accident brought attention to the need for further improvement of I&C functional safety - ability of correct performance of all functions important to safety and corresponding required characteristics in all design modes an operating conditions, operational events, design basis accidents and beyond design basis accidents. For this purpose, NPP safety reassessments, including functional safety of I&C systems and their components, is underway now (Yastrebenetsky, Rozen, Gromov, et al 2011; Yastrebenetsky, Rozen, Klevtsov, et al, 2012).

1. One of the most important directions is equipment seismic qualification for extreme mechanical influences caused by earthquakes (IEC, 1989). I&C seismic qualification has to involve operating stand-alone parts of safety systems and safety system support features, e,g. diesel-generator control systems. It is necessary to estimate influence of seismic

actions not only on devices but also on their fastening to the building constructions, and also on external electric and optical cables in the places of their joining to the device.

2. Not less actual task is assess risk of mistakes of I&C systems and their components, which detect internal and external hazards that could lead to extreme influences to NPP equipment and initiate actuation of systems for prevention and minimization of these influences. Example of these components are seismic sensors, which detect exceeding of regulated accelerating level and generate signal for actuation of emergency and preventive reactor protection system, refueling machine control system, etc. The subject of special study is standardization of accuracy characteristics of seismic sensors and methods of their testing for different forms of seismic acceleration spectra.
3. Dangerous internal events also include ignition in NPP areas, especially in the rooms where safety systems equipment is located. One of directions of fire safety improvement is equipment of NPPs with not only information systems of fire alrm, but control systems of automatic firefighting. These systems have to satisfy requirements on functional safety as the other I&C systems of safety class 2(A) and special safety regulation (NAPB, 2002). Example of these systems designed by Ukrainian companies is complex for fire alarm and control of automatic firefighting SPS1 (Bachmatch, 2008).
4. In addition, it is necessary to reassess components of other I&C systems important to safety in accordance to fire-prevention standards NAPB, 2002. Important task is also estimation of resistance of operating safety class 2(A) stand - alone devices to influence of extinguishing agent, filling a room after actuation of an automatic fire fighting system.
5. Requirements on resistance to temperature influence (see Chapter 3) were formed to prevent violation of operation conditions in the rooms, where operating stand-alone devices are located, and determine time of maximum duration of this influence. This time depend from reason of violation (e.g. LOCA, failure of ventilation, failure of air condition, etc.). Experience shown that time to violation liquidation and restore of operation conditions not exceed time mentioned in Chapter 3. But it is true only in the case when violation cause by one independent event. If violation is a consequence of the other event (e.g. earthquake), more time is needed for restoration of operation conditions. During this time I&C safety systems have to fulfill their functions in high temperature conditions. This take place for another external influencing factors (EIF). No limitation of duration of safety equipment operation at extreme value of temperature (and other EIF) have to be considered.
6. The Fukushima-1 accident showed the need to create post-accident monitoring systems at every NPP, as one of immediate tasks. The post-accident monitoring system (see Chapter 3) should support NPP personnel and safety experts in the control of accidents, mitigation of their consequences, return of the reactor facility to controllable state and subsequent analysis of the causes and progression of design basis and beyond design basis accidents.

The post-accident monitoring system should provide acquisition, archiving, saving, displaying and registration of the following information:

- About character and time of the beginning of initiating events, passing out of operational limits and conditions, incidents and accidents.

- About commands of protective actions initiated by the safety systems and actions of the personnel directed to safety assurance.
- About state of structures, systems and components important for safety, about values of technological parameters and radiation conditions at the beginning or during the mitigation of incidents, passing of the accident and post-accident period.

Ukrainian organizations fulfilled the first steps in elaboration of post-accident monitoring system. The operator (National Nuclear Energy Generating Company) prepared terms of reference and started development of pilot designs of the post-accident monitoring system to be implemented at each NPP.

CONCLUSION

After 2001 Ukraine passed from a country that imported I&C systems for its own NPPs and became a country that not only satisfies own needs, but exports these systems. Some features peculiar to the strategy for NPP I&C modernization in Ukraine may be of interest to specialists from other countries:

- Use of an aggregate of hardware, software and service apparatus called «hardware-software complex» (HSC) as the central part of systems.
- HSC are delivered to NPPs in full assembly, after checkout and testing, with high level of factory availability, what can decrease time to replacement for modernization.
- Use of field programmable gate array (FPGA) for performance of safety functions, including reactor protection systems.

Overall I&C system is considered as a set of interacting individual I&C systems, which implement automatic control of NPP unit technological processes and equipment in all operating modes, automatic protection of systems, equipment and unit as whole, monitoring of non-exceeding of margins of operation and safe operation limits. Reactor control and protection system (RC&PS) is singled out. The overall I&C system includes a set of closely interconnected individual I&C systems, which fulfill control of processes in nuclear reactor. The distribution of functions between I&C systems, included in RC&PS, and interconnections these systems and connections with the other parts of overall I&C system accepted on Ukrainian NPPs is described.

Information which was described in this chapter is recommended for use in safety analysis of NPPs and in elaboration of conceptual technical decisions in implementation of overall I&C systems for new NPP units with WWER-1000 reactors.

REFERENCES

Adamov, E. O. et al. (2005). *Nuclear engineering: Encyclopedia*. Moscow: Mashinostroenie.

Bachmatch, E., Marshevsky, M., Rozen, Y., et al. (2008). Assurance and safety assessment of fire-alarm systems and automatic fire extinguishing in the accommodations NPP. *Nuclear and Radiation Safety, 1*.

Bessalov, G. et al. (2004). *Middle power WWER reactors*. Moscow: Akademkniga.

Brenman, O., Denning, R., et al. (2006). Licensing review of foreign I&C systems for Ukrainian nuclear power plants. In *Proceedings of International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies-5*. Albuquerque, NM: Academic Press.

GND 306.7.02/2.041. (2000) *Methodic of assessment of compliance of I & C systems to safety requirements*. Kiev, Ukraine: State Nuclear Regulatory Committee.

IAEA (1997). *Safety problems of nuclear power plants with WWER-1000/320 reactors (IAEA EBP-WWER-05)*. Vienna, Austria: IAEA.

IAEA (1999). *Modern instrumentation and control for nuclear power plants: Guidebook (Technical reports series, Nº387)*. Vienna, Austria: IAEA.

IAEA. (2002). NS-G-1.3. *Instrumentation and control systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IEC. (1989). IEC 60980. *Recommended practice for seismic qualification of electrical equipment for nuclear power generating stations*.

IEC (2011). IEC 61513. *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*.

Makhutov, N. et al. (2009). *Risk analysis and safety improving of water-water power reactors*. Moscow: Nauka.

NARB (2000). *Fire protection: Firefighting norms development of nuclear power plants with pressured water reactors*. Kiev, Ukraine: Ministry of Fuel and Energy.

Nikituk, V. et al. (2004). *WWER reactors SUZ drives for nuclear power plants*. Moscow: Akademkniga.

Nosovsky, A., Vasilchenko, V., & Pavlenko, A. et al. (2006). *Safety of nuclear power plants: Introduction into safety of nuclear technology*. Kiev, Ukraine: Technika.

NP (2000). NP 306.5.02/3.035. *Requirements for nuclear and radiation safety information and control systems important to safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2003). *Requirements to order and contents to life extension of instruments which included to safety important systems*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP (2008). NP 306.2.141. *General provisions on the safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Committee.

Ostreikovsky, V., & Shviraev, Y. (2008). *Safety of nuclear power plants: Probability analysis*. Moscow: Fizmatlit.

Plutinsky, V., & Pogorelov, B. (1983). *Automatic control and protection of NPP. heat-energetic installation*. Moscow: Energy.

Rezepov, V. et al. (2004). *VVER-1000 reactors for nuclear power plants*. Moscow: Akademkniga.

Samoilov, O. et al. (1989). *Safety of nuclear energetical installation*. Moscow: Energoizdat.

Yastrebenetsky, M. et al. (2004). *Safety of nuclear power plants: Instrumentation and control system*. Kiev, Ukraine: Technika.

Yastrebenetsky, M., Rozen, Y., Gromov, G., et al. (2011). *Requirements to instrumentation and control systems according results of analysis of Fukushima-1 accident*. Nuclear and Radiation Safety, 4.

Yastrebenetsky, M., Rozen, Y., Klevtsov, A., et al. (2012). *Fukushima accident lessons for I&C systems.* Paper presented at the 8th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies (NPIC & HMIT). San Diego, CA.

Yastrebenetsky, M., Rozen, Y., Siora, A., et al. (2010). *Ukrainian NPP I&C regulatory framework: Elaboration and application*. Paper presented at the International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies-7. Las Vegas, NV.

ADDITIONAL READING

Bakhmach, E., Siora, A., Bezsalyi, V., & Yastrebenetsky, M. *Digital systems for reactor control: design, experience of operation.* Proceedings of the 16 th International Conference on Nuclear Engineering ICONE16, 2008, Orlando, Florida, USA.

(2011). *Core knowledge on instrumentation and control systems in nuclear power plants. IAEA nuclear energy series, No. NP-T-3.12*. Vienna, Austria: IAEA.

EPRI. (2005). *1011851. Guidance for the Design and Use of Automation in Nuclear Power Plants*. Palo Alto, CA, USA: Electric Power Research Institute.

EPRI. (2010). *1015313. Computerized Procedure Systems: Guidance on the Design, Implementation, and Use of Computerized Procedure Systems, Associated Automation, and Soft Controls*. Palo Alto, CA, USA: Electric Power Research Institute.

Kharchenko, V., & Sklyar, V. (Eds.). FPGA-based NPP. Instrumentation and Control Systems: Development and Safety Assessment. Research and Production Corporation Radiy, National Aerospace University KhAI, State Scientific and Technical Center for Nuclear and Radiation Safety. Kirovograd – Kharkov, 2008.

KEY TERMS AND DEFINITIONS

Control and Protection System: A complex of interconnected safety and normal operation I&C systems, providing safety control of a chain nuclear fission reaction.

Control Area: A territory that may be affected by radioactive releases and discharges from NPP and where radiation monitoring is conducted.

Control Element: A reactivity control feature that contains control rods with drives and neutron absorbers (absorber rods) which can be transferred in the reactor core.

Emergency Protection: I&C function intended for rapid transfer and long-term support of the reactor core in a subcritical state, that is characterized by the effective multiplication factor whose value is to be less than one, and a lack of local criticality.

Facilities of Influence on Reactivity: Hardware that provides change of core reactivity due to change in position of neutron solid sorbents or density change of fluid sorbents.

Modernization: Set of actions for improvement of safety, functional abilities, reliability and/or technical and economic measures of an active I&C system, connected with replacement of separate components by more up-to-date ones, which requires changes to the accepted design and / or operational documentation. (The same term is "modification").

Preventive Protection: I&C function intended for limitation or decrease of the reactor power to a safe level in case of operational events.

Primary Circuit: A piping system, technological facilities, systems and elements intended for circulation of the coolant through the reactor core in operation modes and conditions specified by the design.

Reactor Core: A part of the reactor facility, in which nuclear fuel, moderator, absorber, coolant, facilities, having an influence on reactivity and structural elements, intended for a controlled chain fission reaction and transmission of energy to the coolant, are located.

Reactor Facility: A Complex of structures, systems and components intended for conversation of nuclear energy into thermal energy, including a nuclear reactor, elements of the primary circuit, emergency protection and proper I&C systems of safety and normal operation and a nuclear fuel reloading system.

Chapter 9
Emergency and Preventive Reactor Protection Systems

Yuri Rozen
State Scientific and Technical Center of Nuclear and Radiation Safety, Ukraine

Svetlana Vinogradska
State Scientific and Technical Center of Nuclear and Radiation Safety, Ukraine

Alexander Siora
Research and Production Corporation Radiy, Ukraine

ABSTRACT

In Chapter 9, Emergency and Preventive Reactor Protection (E&PRP) systems implemented at the Ukrainian NPPs during 2003-2013 are considered. The core of E&PRP systems is formed by software-hardware complexes (SHC E&PRP) developed on the base of the Research and Production Corporation "Radiy" equipment family. The first part describes the main purposes of E&PRP: forced power reduction or immediate reactor shutdown to prevent an emergency from developing into an accident. The second part describes the basic functions determined by the system purposes, along with additional functions performed by SHC E&PRP. The third part is devoted to describe SHC E&PRP technical characteristics, which implement the specified functions. The forth part deals with information about the composition and structure of SHC E&PRP, as well as about connections of SHC E&PRP with adjacent I & C systems are shown. In the fifth part, aspects of functional safety assurance during development, production, and acceptance of SHC E&PRP are considered.

INTRODUCTION

SHC E&PRPs used as a technical base in the reconstruction of existing and creation of new emergency and preventive reactor protection systems, perform the following:

- The data storing on provided by the design operational limits and conditions of the normal and safe unit operation, ERP and PRP algorithms of control signal (commands) forming, which initiate the actuation of emergency or preventive reactor protection accordingly;

DOI: 10.4018/978-1-4666-5133-3.ch009

- The reception of technological process control parameters and equipment condition data from sensors and/or adjacent instrumentation and control systems;
- The forming and output from ERP or PRP commands to adjacent I&C systems in case of any conditions regimented in the appropriate algorithms of emergency or preventive reactor protection;
- The archiving, display and data registration on the technological process controlled parameters, equipment condition, reactor protections actuations, and the reasons of such actuations;
- The continuous monitoring (diagnostics) of its technical state, fault detection and identification, archiving, display and registration of diagnostics results;
- The data output into unit computer information system (CIS) and personnel warning facilities in the main control room.

The preventive reactor protection is the function of normal operation (category B), aimed to prevent the possibility of emergency in case of the deviation of technological process parameters beyond the admissible operational limits and/or in case of normal operation conditions violation set by the project. It is achieved by forced power reduction and / or blocking of any commands, which could initiate power increase.

The emergency reactor protection belongs to the safety functions (category A) and activates in the case of the violation of the provided design limits or conditions, which cannot be eliminated with the help of a relevant systems of normal operation (e.g., due to its failure), or in the case of the events, which could lead to technical parameters variation, being too fast for adequate response of the systems of normal operation, and also in case of violation of unit design conditions safety operation. In such cases, ERP command should be output, which initiates simultaneous insertion of all control rods into the core, causing a reactor subcritical state and power unit shutdown. It defines an essential role of the emergency reactor protection in NPP safety assurance as the last way to avoid the accident.

On the other hand, the cost of "false" power unit shutdowns (unnecessary) due to false operation of the emergency reactor protection, which can be the result of failure or SHC E&PRP malfunction, is obvious.

It would lead to the necessity to regulate the technical specification in such a way to provide quality of the development, production, testing and operation of SHC E&PRP, which correspond to its role in safety assurance, and to make certain that such correspondence is actually achieved. Thus, one of the fundamental safety principles was considered, according to which I&C systems and its equipment should be designed, produced and maintained in such a way, that their specification, verification and validation, quality assurance, quality control and reliability met their safety classification.

BACKGROUND

Chapter 9 provides a short description of the devices and systems performance, which fulfill emergency and preventive reactor protection functions, being a part of the reactor control and protection system at the Ukrainian NPPs. This chapter provides more detailed information about the purpose, performed functions, technical specifications, composition and structure of E&PRP systems, as well as functional safety assurance on the system life cycle stages.

The requirements to E&PRP systems and SHC E&PRP are determined by common properties of safety important I&C systems and their components, outlined in Chapter 3, and consider the purpose, categories of performed functions and safety class.

PURPOSE

Emergency reactor protection system (other names- reactor trip system, scram system) should provide safety in the cases, when the systems of normal operation fail to keep power unit technical parameters within the specified design limits. The reasons of this can be a failure of one of the control system of normal operation main functions or a specific event, which could lead to technological process parameters variation, being too fast for adequate response of systems of normal operation. In such cases, in order to prevent emergency and/or accident, an immediate reactor shutdown may be required (chain reaction termination and maintenance of the reactor in a safe state), which is performed by the relevant safety systems performing emergency protection function. Reactor shutdown may be required also for the mitigation of the accidents.

The failure of emergency protection function can lead to nuclear accident with radioactive release beyond the project specified limits in the amount exceeding the determined norms of radiation exposure on the personnel, population and environment. At the same time, false actuation of emergency protection in the absence of hazardous conditions leads to substantial economic loses due to the unit shutdown, which can resume operation only after the analysis of the actuation reason and after obtaining permission to start in accordance with the determined procedures.

In case of some design limits violations or conditions of normal operation, emergency can be prevented without the reactor shutdown by reducing its power (sometimes it is enough to forbid power increase). These functions are performed by preventive protection.

FUNCTIONS

Emergency reactor protection (ERP) provides fast termination of chain reaction required in the most severe initial events. Within the subrange controlled during fuel loading, and within start-up subrange the emergency protection is performed if the design limit for neutron flux density is exceeded in each of these subranges. Within the operational subrange, the reasons for the emergency protection actuation are relative level increase of neutron power or decrease of half-life to a specified (maximum or minimum accordingly) limit. The emergency protection is also performed in the cases, when any of the process parameters (pressure over a core, steam line pressure, coolant temperature, steam generator water level, or compensator pressure, etc.) reaches its limit of the set parameter.

For example, if main circulation pumps (MCP) are switched off, decrease of coolant flow can lead to the rise of its temperature, start of vigorous boiling and heat exchange crisis, which, in turn, leads to fuel elements damage. Decrease of pressure over core, caused by pressure compensator malfunctioning, can lead to the same result. To accelerate the response to such violations and to prevent hazardous consequences emergency protection actuation is provided in case of safe operational conditions violations (main circulating pumps deenergizing, loss of primary coolant circuit, power outage on power rails, failure of the system to perform emergency protection function and in the other cases under the design). For example, when switching off two of four operating MCPs (at a power more than 75% of nominal power) or one of two operating MCPs (at a power more than 5% of nominal power) the reactor should be shutdown before the system detect the raise of a coolant temperature caused by these events, as by that time fuel element cladding can be destroyed.

Preventive reactor protection does not allow to increase core power or provides power reduction to a safe level in order to prevent exceeding of operational limits (occurrence of emergency). For example, when the coolant pressure over core rises to 165 kG·cm $^{-2}$, a preventive protection command is formed by which any actions, which could lead to the reactor power improvement, are blocked. If the pressure continues to rise and reaches 172 kG·cm $^{-2}$, the command for power reduction is sent and it lasts until the pressure over core restore to the initial value. And only in case if all the taken measures are not sufficient, when pressure rises further to 180 kG·cm $^{-2}$, the emergency protection actuates and shutdowns the reactor.

Increase of core power is forbidden, for example, in case if relative level of neutron power, half-life, pressure over core exceed set design limits and also in case of dropping of control rods into the core..

Emergency and preventive reactor protection functions are performed by E&PRP system. Its direct task is the initiation of appropriate protective actions. For this purpose, E&PRP system continuously monitors the current values of neutron and technological parameters, and the state of the unit main technological equipment; detects the violations of design limits, safe operation conditions and performs other actions set by the protection operation algorithms; sends safety actions commands (ERP or PRP), which cause the actions by design of adjoin systems; sends signals to the operating personnel about protection actuation and its cause; displays the control parameters, events, conditions, sent commands and their causes. The safety action commands, initiated by E&PRP system, are sent to rod group and individual control (RG&IC) system for execution.

Besides the mentioned main functions determined by the system purpose, the performance of additional functions in a varying degree is provided. They include:

- Continuous monitoring of operability of own hardware and software, cable lines, power supply system, etc.;
- Failure diagnostics, providing the operating personnel with information on violations of operability;
- Memory and storage of data about control parameters, events, states, protective actions commands, causes of protection operation and diagnostic information in the operational and permanent archives; output of archive data for displaying and registration;
- Transmission of current and/or archive information to other power unit systems: CIS, turbine control system (TCS), in-core reactor monitoring system (IRMS), post-accident monitoring system (PAMS), etc.;
- Support of the personnel during the checks on the shutdown reactor, before start and during power unit operation at power (during the process of operational checks and after the restoration).

CHARACTERISTICS

While setting requirements to E&PRP system, it was intended that the emergency reactor protection function refers to category A, the preventive reactor protection- to category B. The components of E&PRP system, involved in emergency protection function performance, are the safety elements and refer to safety class 2(A). The components, involved in performance of preventative protection function, are the elements of normal operation important for safety, and relate to safety class 3(B). The components, which perform additional functions of archiving, displaying, data transfer, monitoring, failure diagnostics, protection testing should be also related to this class. For registration functions, which do not influence to safety directly, the category is not set; components involved in performance of these (and only these) functions are related to class 4. Each E&PRP system combines purpose and functions of safety systems and normal operation and relates to safety class 2(A).

Considering that emergency protection is one of the main emergency prevention means, forming third level of defense-in-depth in accordance with NP, 2008,a the strictest requirements specifically determined by a range of international and national Ukrainian safety regulatory documents should be raised upon it. Requirements to emergency reactor protection function and systems and elements associated with it, are specified in the international standards (e.g., IAEA, 2002; IAEA, 2012), USA standards (e.g. ANSI/IEEE, 1987 and later), rules and regulations, be in force in Ukraine (e.g. NP, 2008b).

The requirements to monitoring and control of process operation functions, in performance of which E&PRP systems are involved, are provided in IAEA, 2012 and NP, 2008,b. It is required to have at least two different and independent systems of reactor shutdown, each of them should provide the transition of the core into subcritical state, in which the value of effective multiplication factor is less than unity and local criticality is absent. One of these systems should perform the emergency protection function and have a fast response sufficient to shutdown the reactor from any operational state not violating normal operation limits. When the reactor is tripped, any unintentional reactivity rise should be prevented, however, the ability of personnel reasonable actions (such as refueling, diluting of boron solution, neutron poison flow during maintenance, etc.) leading to raise of reactivity in standby mode, has not to block (IAEA, 2012).

The emergency reactor protection should be carried out according to neutron flux density level and the speed of its growth, and should be provided over the whole range of neutron flux density change (from 10^{-7}% to 120% of the nominal value). Other parameters, according to which the emergency protection should be performed, are determined in accordance with reactor system design. The list of such parameters, set-points and conditions of scrams should be substantiated in the design in such a way to exclude the possibility of safety limits violation.

The action started by emergency reactor protection should be fully performed. Control rods (CR), which provide reactor shutdown, should be operated from any working or intermediate positions. IAEA, 2012 provides a possibility of usage of CR part to reactivity control (for example, to regulate neutron reactor power) in normal operation modes, provided that the possibility to core shift to subcritical state is supported regularly and with a proper allowance. All regulations and standards point at the necessity to monitor the availability of emergency function performance, including the possibility of checking of the protective actions commands formation and the time required for their passing (without affecting CR).

In case of normal operation violations, when the emergency reactor protection scram is not required, preventive reactor protection is applied.

In accordance with NP, 2008,b the emergency reactor protection (ERP) system should be separated from other I&C systems, in order for the damages or any element removal of these systems not to influence the ability of ERP system to perform its functions. Upon combining of emergency reactor protection and normal operation functions in one system, the priority of emergency reactor protection should be provided and should be shown that such combination will not lead to violation of safety requirements and deterioration of elements' reliability, performing emergency reactor protection functions. If the same signals are used in ERP system and any other I&C system, an appropriate separation should be provided (for example, galvanic isolation).

In accordance with IAEA, 2002 and IAEA, 2012, the redundancy and the independence embedded into ERP system design, should be sufficient to provide that (1) none of single failure will not lead to loss of protective function and (2) removal of any component or channel will not lead to the loss of required minimum redundancy. Regulations NP, 2000 and NP, 2008,b define redundancy requirements that emergency reactor protection system should consist at least of two independent sets, each of them should be designed in a way that emergency reactor protection was provided by not less than 3 independent channels on neutron flux density level, neutron flux density changing period, and on each technological parameter. It is provided that ERP command should be formed upon coincidence of signals in, at least, two of three channels. The use of such a redundancy principle providing fulfilling the specified requirements to system reliability (concerning emergency protection failure), at the same time facilitates reducing of false actuation probabilities, which can lead to the reactor shutdown in nonhazardous situations.

IAEA, 2002 and IAEA, 2012 international standards recommend to specify measures which minimize the probability of operator's actions that can damage the effective operation of protection system under normal operation and expected operational event, but that do not prevent operator's appropriate actions in case of design accident. NP, 2008,b regulations require to provide monitoring and operability diagnostics of channels and sets with displaying of fault information and forming emergency protection or alarm signals in case of sets or channels failure. There is also stated that in case or the failure or the removal of one channel in the operating emergency protection set, the emergency protection signal should be formed automatically at the channel output.

In accordance with IAEA, 2012 during operation protection system should permit periodic checking of each set operability with the operating reactor. Aim of the testing is to check compliance with design characteristics and to detect faults, which could happen after the previous testing and lead to partial or full loss of redundancy (NP 2008,b). Periodical tests should cover all the system components engaged in protective function performance, from sensors to respective actuating systems or equipment inputs. The requirements to removal of one set or one set channel (allowable reactor power level limit, condition of other units, potential duration, etc.) should be defined and reasoned in a way to minimize the possibility of any negative impact on operation and power unit safety condition. The possibility of set or emergency protection channel removal without power unit personnel warning should be excluded with the help of the proper technical equipment.

The main component of E&PRP system is software-hardware complex (SHC), which is engaged in performance of all its main and additional functions.

The requirements to software-hardware complexes emergency and preventative reactor protection (SHC E&PRP) result from:

- General requirements to operation, reliability, durability, quality and independence of performed functions, applied to safety class 2(A) components and their operationally-autonomous component parts;
- Specific requirements to redundancy methods (structure), independence, diagnostics and controllability of emergency protection and preventative protection systems.

The diversity requirement directly and exclusively relates to SHC E&PRP. Complexity and uniqueness of each SHC as a single product, which is developed (or updated) for a specific system, increase the risk of hidden faults, being not detected during validation or acceptance testing. Hidden faults made during the development, configuration, and / or production of SHC E&PRP, can appear in the process of performance as a common cause of redundant channel fault in both sets. Taking into account these features, IAEA, 2012 standard recommends to use functional diversity maximally, as well as a diversity of technical and program means or operation principles to prevent the loss of protective function (characteristics of possible diversity kinds are described in Chapter 3).

It is pertinent to note that diversity requirement is less actual with regard to the peripheral (as a rule, industrial) items, as a major part of faults can be detected and eliminated at the development stage, and properties of developed and industrial items can be fully checked and validated during testing. Moreover, as a rule, the utilized peripheral items approbated by a long-term practice of operation at NPPs to an adequate degree (different systems use same type sensors, normalizing transducers, actuators, and other peripheral equipment), that is why during modernization of I&C systems most often only central part (SHC) is changed, peripheral equipment of the modernized system and connecting cables are not changed often.

Regulations NP, 2000 and NP, 2008,b provide requirements for obligatoriness of system diversity performing reactor emergency protection (shutdown) function, while for I&C systems and SHC, which are not engaged in emergency protection function performance, requirement for observance of diversity principle is not obligatory, but can be set by the operating organization. At the same time, international standard IAEA, 2002 provides a possibility of diversity usage not only in safety systems, but also in normal operation systems along with other measures of additional reliability growth, and also as a way of compensation of difficulties, which appear if there is a need to prove a reliability of, for example, reserved and (or) computer systems, reliability of which can be restricted by such factors as common cause failures. Design defects, production defects, operating errors and maintenance errors are said to be the most probable reasons of such failures. Similar recommendations concerning usage of diversity as a way of effective error protection (especially for complex systems, which are not enough approbated during operation) are provide, for example, in IEC, 2006 and IEC, 2011 standards. However, IEC, 2009 specifies that the usage of two or more systems, built on different principles is necessary, if a really achievable reliability of category A functions and equipment connected to it, taking into account the common cause failures, cannot provide the safety performance requirements. Diversity requirement applicable to safety control systems is also included into USA documents (NUREG, 2002), Russia (NP, 1997), Germany (KTA, 1985) and implemented, for example, in emergency protection systems at Sizewell B NPP (UK) new power units, Temelin NPP (Czech Republic), etc., as well as during modernization of E&PRP systems at Ukrainian power units.

CONSTRUCTION PRINCIPLES

For WWER-1000 reactors, the design provides four types of protection.

Emergency reactor protection (ERP) initiates the disconnecting of power supply of all control rod drives that leads to their simultaneous falling into the lowermost position driven by their own weight, which, in turn, causes fast (within 1.5 s-4 s) transition of the reactor in subcritical state. The subcritical state remains even after the elimination of the conditions that caused ERP actuation until the personnel send command ERP RESTART.

Reactor accelerated preventive protection (RAPP) operates, when the nuclear reactor power is 75% over the nominal. RAPP increases the power unit dynamic resistance and provides reactor sparing regimen in case of abnormal disconnection of technical equipment due to fast power reduction. For this purpose, RAPP initiates CR drives disconnecting of power supply of the previously selected CR group that causes simultaneous fall of all constituent control rods and, due to this, fast (within 1.5 s—4 s) power reduction to 30%—40% of the nominal. At the same time the signal is sent (with a 4 s delay) to turbine control system (TCS) upon which turbogenerator power is reduced to (350-450) MW level with the speed (20-30) MW·s $^{-1}$. The lift of dropped CR is possible only after the personnel send a special command RAPP RESTART. CR group, which should perform reactor accelerated preventive protection, is selected before each fuel campaign considering core loading.

Preventive reactor protection PRP1 causes successive lowering of CR groups in the design sequence with working speed 20 mm·s $^{-1}$. An exception is the fifth group (used for xenon oscillation suppression, the movement of which is not provided by the PRP1 commands). Lowering of CR groups into core leads reactor power reduction (during PRP1 performance the automatic power control is switched off). When the conditions of the protection actuation are eliminated, PRP1 command is cancelled and CR groups lowering is stopped.

Preventive reactor protection PRP2 forbids the increase of reactor power, i.e. upward movement of any CR or CR group (except the fifth one). When the conditions set for the protection actuation are eliminated, PRP2 command is cancelled and, thus, allows to increase the reactor power.

Initialization of commands of emergency reactor protection and preventive reactor protection realizes by software-hardware complex SHC E&PRP, Initialization of commands of reactor accelerated preventive protection - by software-hardware complex SHC RPwCUL&APP (see Chapter 8). The actuation system, which performs functions, initiated by noted commands, is rod group and individual control (RG&IC) system (see Chapter 10).

Conditions of protection actuation are determined by the design for each power unit. They had some differences for different power units caused, in particular, by the features of used neutron flux monitoring system (sending signals on exceeding of neutron power setpoints and the neutron half-life), and also differences in the limit parameters, which determine conditions of protection actuation).

The design determines the limits of power level and unit operating time in case of failure of emergency and preventive equipment:

- Failure of one set of SHC E&PRP, leading to impossibility of emergency reactor protection function Initialization by this set and / or removal of one set of SHC E&PRP: power level is not restricted, operating time is not more than 8 hours;
- Failure of one channel in one of SHC E&PRP sets: power level is not restricted, operating time is not more than 8 hours;
- Failure of indication of reason alarm ERP in one of the SHC ERP sets: power level is not restricted, operating time is not more than 8 hours;
- Failure of two set SHC E&PRP leading to impossibility of PRP1 function Initialization: power level is not more than 50% of the nominal, operating time is not more than 8 hours;
- Failure of indication of reason alarm in two SHC E&PRP sets: operation on power is forbidden.

Upon the expiration of allowable operating time and before the elimination of the fault, the unit shutdown was provided, during which the technological equipment is in an availability state, its parameters are close to operational parameters, and it is required 2-3 hours to gain power.

Technical solutions applied in a typical design (before modernization) of WWER-1000 reactor protection system, was based on unconditional ("hard wired") logic principles implemented on micropower (KMOS) integrated circuits and did not provide the use of programmed computing systems (e.g. microprocessors, etc.) for the implementation of the specified functions.

From the other principles of the typical design it is primarily required to mention the ones that remain also in the new reactor protection systems:

- Presence of two SHC sets located in different rooms and completely autonomous, each of them can perform all protection functions provided by the design;

- Three-channel structure of each set using logical condition “two of three” while forming protection commands on independent channels signals;
- Primary use of parametrical discrete signal (in form of low and high resistance of electric circuit, receiving energy from the load) and logical agreement, on which signal active state is represented by high resistance of the chain (for example, breaking of normally opened contacts due to output relay winding disconnecting of power supply);
- Electric power supply of each set from three autonomous sources, duplication of secondary feed block in each channel and their connection to reliable power sources, according to scheme allowing to save set capacity in case of loss of one or two sources.

Since 2003 the modernization of the current emergency and preventative reactor protection systems at Ukrainian NPPs had started. The technical base of modernization was equipment family (platform), developed by Research and Production Corporation “Radiy” (Bachmatch, 2008), and software-hardware complexes of emergency and preventive reactor protection were created on its base. In 2004-2005 SHC E&PRP were produced and delivered for power unit 4 Rovno NPP. In 2007-2009 according to the European Union program of Technical Assistance for the Commonwealth of Independent States (TACIS) the modernization of power unit 1 reactor control & protection system at Khmelnitsky NPP was performed.

SHC E&PRP (Figure 1) consists of two autonomous functionally identical sets, each of them can be removed for performance testing (control and indicating signals forming accuracy in case of imitation of limits and safety performance violations).

Each set is designed in a form of operationally autonomous component parts combination, which are connected on-site by electrical and optical communication links. The set includes:

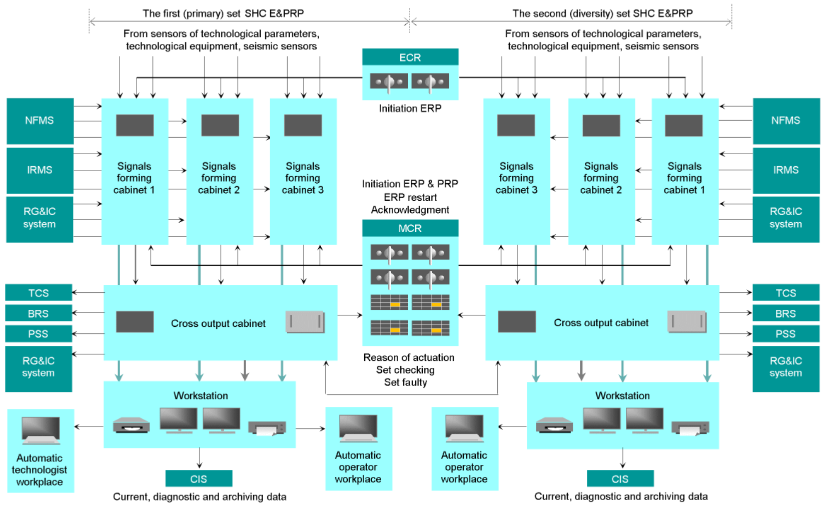
- Three identical signal forming cabinets, which form three autonomous inter-redundant protection channels;
- Cross output cabinet, which form set output signals basing on data received from three signal forming cabinets;
- Workstation which performs data archiving, displaying and registration;
- Automated operator workplace intended for displaying of control parameters, condition of discrete input and output, as well as the reasons of protection actuation.

The common feature for both sets is automated technologist workplace where the operability testing of SHC E&PRP parts can be carried out, as well as set-points change.

Each signal forming cabinet receives the required data in form of continuous electrical and discrete signals from its “own” sensors set and software-hardware complex adjacent I&C systems: neutron flux monitoring system (NFMS), in-core reactor monitoring system (IRMS), rod group and individual control (RG&IC) system, as well as from seismic sensors. The signals from these sources are connected to signal forming cabinet via intermediate terminal blocks cabinet. Construction of terminal blocks allows to send test impacts imitating input signals from the test bench without external cables disconnection.

The output control and indicating signals are sent via communication lines to the cross output cabinet from each signal forming cabinet. After the signals processing according to logical condition “two or more of three”, ERP commands form in the cross output cabinet of each set and they are transferred via communication lines to RG&IC system, turbine control system (TCS), boron regulation system (BRS), power supply system of control rod drives (PSS). PRP commands are formed according to a logical

Figure 1. Software-hardware complex of emergency and preventive reactor protection system (SHC E&PRP)


The first (primary) set SHC E&PRP
The second (diversity) set SHC E&PRP
From sensors of technological parameters, technological equipment, seismic sensors
From sensors of technological parameters, technological equipment, seismic sensors
ECR
Initiation ERP
NFMS
IRMS
RG&IC system
Signals forming cabinet 1
Signals forming cabinet 2
Signals forming cabinet 3
Initiation ERP & PRP
ERP restart
Acknowledgment
MCR
Signals forming cabinet 3
Signals forming cabinet 2
Signals forming cabinet 1
NFMS
IRMS
RG&IC system
TCS
BRS
PSS
RG&IC system
Cross output cabinet
Reason of actuation
Set checking
Set faulty
Cross output cabinet
TCS
BRS
PSS
RG&IC system
Workstation
Automatic technologist workplace
CIS
Current, diagnostic and archiving data
Automatic operator workplace
Automatic operator workplace
Workstation
CIS
Current, diagnostic and archiving data

condition "two of three" and are transferred via communication lines to RG&IC system, TCS and RPwCUL&APP system from the cross output cabinet of each set (not represented in Figure 1). The possibility of current, diagnostic and archived data output from workstation to CIS is provided.

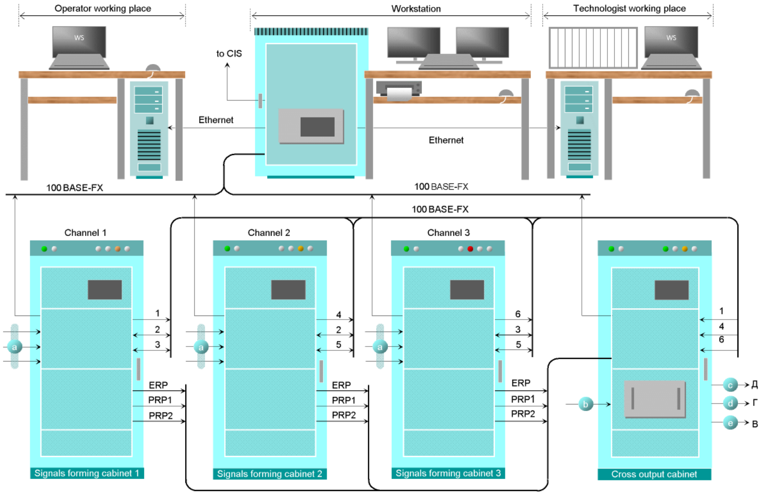
The components of SHC E&PRP set and interconnections are shown at Figure 2.

For digital message exchange between signal forming cabinets and transfer of messages that forms in signal forming cabinets and the cross output cabinet to workstation, local networks with 100BASE-FX interface and end-to-end topology are used, shown in Figure 2. Automated operator and technologist workplaces are connected to Workstation according to the standard serial digital data channel (usually one of the Ethernet network variants), which is supported by Workstation server and Industrial PC, on which base the automated operator and technologist workplaces are implemented. The way of workstation connection to CIS is defined for each power unit with regard to data input interface used for the current CIS.

Signal forming cabinet performs:

- Reception of direct current analog signals:
  - ◦ From pressure sensors, pressure differential sensors, level sensors;
  - ◦ From normalizing transducers of power and frequency alternating current powering main coolant pumps;
  - ◦ From thermoelectric transducers (low voltage direct current);
- Reception of discrete signals:
  - ◦ From NFMS (excess of neutron power values and decrease of power change period);
  - ◦ From the voltage monitoring equipment on the first and second alternating current input 380 V (power supply loss);
  - ◦ From IRMS (decrease permissible reserve to boiling crisis on the fuel element surface, excess of local power density limit, coolant temperature raise on the outputs of individual fuel assemblies over the limit);
  - ◦ From RG&IC system (insertion of at least one of CR into the core);

Figure 2. Structure and configuration of SHC E&PRP set



    - From seismic sensors (earthquake detection with intensity above the limit);
- Computation of parameter values which cannot be measured directly, for example, differences of first and second circuits saturation temperatures (further – design values);
- Storing of data:
    - On control parameters limits;
    - On conditions of normal and safe power unit performance;
    - On signal forming algorithms, initiating actuation emergency and preventive reactor protection in case of violation of these conditions or exceeding the set limits;
- Forming in accordance with the algorithm and sending to cross output cabinet of control signals (commands ERP or PRP1, PRP2) in case of detection of any emergency or preventive reactor protection actuation conditions (depending on conditions caused system actuation, the control signal delay and / or automatic signal withdrawal after the set time delay are provided);
- Receiving of commands from the control keys located in the main control room and the emergency control room, that initiate:
    - Accident and protection systems actuation;
    - Return to normal position after emergency protection actuation;
    - Display switch-off that indicates the actuation reason.

Additional functions of signal forming cabinets:

- Continuous monitoring of technical state condition of its hardware, adjacent equipment and signal and message lines;
- Forming and sending to workstation of digital messages which contain information on the current monitoring parameters values, initial events, state of technological equipment and diagnostics results;
- Setting and changing of the control parameters limits.

Structural scheme of signal forming cabinet are shown at Figure 3.

The cabinet consists of: sensors power supply crates (connected supply blocks and panel computer); signal processing crates; two relay output crates; power supply crates.

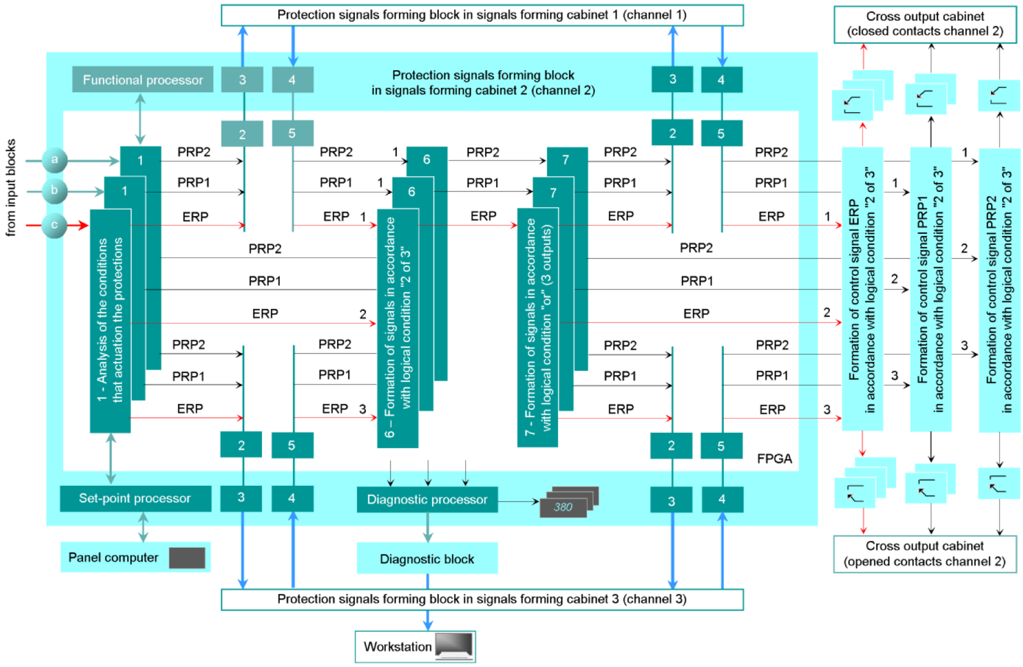
In the *signal processing crate* data entry blocks are structurally and electrically connected, they provide:

- Input and normalization of discrete signals;
- Input and conversion of continuous direct-current signals;
- Input and conversion thermoelectric converters natural signals;
- Processing of the received data and forming of control signals (commands);
- Monitoring of technical state and diagnostics of cabinet, transmission lines and adjacent equipment failures.

Protection signals forming block performs (numerical symbols in brackets correspond to symbols at the respective schemes in Figure 3):

- Signal receiving, received data processing, control of set conditions for emergency and preventative protection actuation (1);
- Forming (in accordance with the regimented network protocol) of digital messages, containing data received from input blocks, as well as identifiers of protection actuation conditions, if these conditions were detected (2);
- Conversion of digital messages electrical elements into optical (3) and transition of messages via fiber-optical communication lines to protection signals forming blocks in two other channels (signals forming cabinets);
- Receiving of similar messages from protection signals forming blocks of two other channels, conversion of optical elements into electrical (4) and decoding of the received digital messages in accordance with the regimented network protocol (5);
- Comparison of messages received from input blocks and from two other channels, detection of discrepancies, forming and

Figure 3. Structure scheme of signals forming cabinet (1-st set, channel 2)



Protection signals forming block in signals forming cabinet 1 (channel 1)
Cross output cabinet (closed contacts channel 2)
Functional processor
Protection signals forming block in signals forming cabinet 2 (channel 2)
from input blocks
a
b
c
1 - Analysis of the conditions that actuation the protections
6 – Formation of signals in accordance with logical condition "2 of 3"
7 - Formation of signals in accordance with logical condition "or" (3 outputs)
Formation of control signal ERP in accordance with logical condition "2 of 3"
Formation of control signal PRP1 in accordance with logical condition "2 of 3"
Formation of control signal PRP2 in accordance with logical condition "2 of 3"
PRP2
PRP1
ERP
1
2
3
4
5
6
7
FPGA
Set-point processor
Diagnostic processor
380
Panel computer
Diagnostic block
Protection signals forming block in signals forming cabinet 3 (channel 3)
Workstation
Cross output cabinet (opened contacts channel 2)

sending of diagnostic messages to the diagnostic block (not represented in Figure3);

- The first level of logical processing: forming of ERP, PRP1 and / or PRP2 signals if the same actuation condition was detected by, at least, any two channels (6): quantity of outputs is equal to quantity of actuation conditions for the respective kind of protection;
- Forming of output ERP, PRP1 or PRP2 signal if, at least, one of the emergency reactor protection actuation condition was identified, or one of preventive reactor protection PRP1 actuation condition, or one of preventive reactor protection PRP2 (7) actuation condition was identified;
- Forming of digital message, containing data identification of protection actuation conditions (2), conversion of electrical elements into optical (3) and transition of messages in two other channels;
- Receiving of similar messages from two other channels, conversion of optical elements into electrical (4), decoding of the received digital messages (5) and forming of output ERP, PRP1 or PRP2 signal.

The main part of protection signals forming block functions performs field programmable gate array (FPGA), which structure, besides the above mentioned 1, 2, 5, 6 and 7 elements, comprises functional processor, set-point processor and diagnostic processor.

The output signals from the protection signals forming block are sent to the blocks formation of control signal, installed in *relay output crates*. Each of these blocks receives signals of one type (ERP, PRP1, PRP2) from the first, second and third channels and forms output signal, if such signals were received from any two or all three channels (the second level of logical processing). Signal multiplication blocks installed in relay output crates are relay repeaters of the received discrete signals. In the absence of signal, all relays in the blocks are energized; appearance of a signal leads to relay de-energize, opening of normally closed contacts and closing of normally opened contacts, that is interpreted as the emergency or preventive protection control signal at the respective channel output. The control signals at the other two channels output are formed in the same way.

Cross output cabinet performs the third level of logical processing. If ERP, PRP1 or PRP2 signals received from two or three channels, at its outputs form the commands (in form of discrete signals) which initiate actuation of:

- Emergency protection:
  - of rod group and individual control system (de-energize of CR drives);
  - of power supply system of control rod drives (removal of base and reserve supply from the CR drives);
  - of turbine control system (turbine removal of load);
  - of boron regulation system (boron pump switch-off);
- Preventive protection PRP1:
  - of rod group and individual control system (unit power reduction by lowering of CR groups with the nominal speed in the design order);
  - of reactor power control, unloading, limitation and accelerated preventive protection system (removal of automatic power control regulation with the consequent switch-on at new power level);
  - of turbine control system (turbine power reduction);
- Preventive protection PRP2:
  - of rod group and individual control system (inhibitory action of CR lift);
  - in reactor power control, unloading, limitation and accelerated preventive protection system (inhibitory action of reactor power expansion);
  - in turbine control system (inhibitory action of turbine power expansion).

ERP, PRP1, PRP2 commands duplicate at cross output cabinet outputs; in this case a separate independent output is provided for each commands receiver and each reserved channel in the receiver (if there are such channels). Cross output cabinet also performs logical processing (according to “two or more of three” condition) and sending of signals to alarm devices, installed in the MCR, which indicate the reasons of protection actuations and set condition (failure, removal for testing or maintenance).

Workstation realized on base of industrial computer or server, performs the receiving of messages from signal forming cabinets and cross output cabinet, accumulating of received data in the operative (hour), day and long-term (up to one year) archives, displaying and registration of the current and archived information.

In order to receive messages from signal forming cabinets and cross output cabinet transmitted via fiber-optic lines, workstation is equipped with USB-OPTO interface adapters which are installed in free positions (slots) and connected to the industrial computer USB-ports.

Workstation displays allow to supervise the condition of each channel input and output signals, sending of ERP, PRP1, PRP2 commands, set operating mode, temperature in three positions in each cabinet, doors opening and shutting, non-fire condition inside the cabinet. The workstations display information is showed in form of technological symbolic circuits, tables, diagrams, text messages. Data are updated not less than one times in two seconds.

SHC E&PRP energy supply is performed directly from NPP auxiliary power (from two interredundant sources) by three-phase alternating current with nominal power 380 / 220 V and frequency 50 Hz. The allowed continuous deviation of the supply voltage is from minus 15% to plus 10%, frequency – from minus 2% to plus 2% of the nominal value. Workstation and automated operator workplace equipment is designed for supply from alternating current with the 220 V nominal voltage and 50 Hz frequency and contain uninterruptible power supply blocks which provide performance within at least hour in case of network outage.

The element base used in SHC E&PRP (operating amplifiers, digital to analog and analog to digital converters, galvanic isolation elements, discrete logical elements, safety systems relay, resettable fuses and others) are purchased in the leading companies (Motorola, Fairchild, Samsung, MAXIM, etc.). For realization of reactor emergency and preventive protection function (receiving of digital data, violation detection, digital messages encryption and decryption, processing according to logical condition “two or more of three”, control signals forming) programmable integrated logic circuit are (FPGA of Apex EP20K200 and Cyclone EP1C12 families ALTERA company). Both FPGA families provide great integration level, high operating speed, low power consumption, which became one of the factors that allowed to provide structure simplicity, compactness and effectivity of SHC E&PRP.

The development of FPGA logical structure is supported by Quartus instrumental designing system (environment) by ALTERA company, with addition of special Cyclone family FPGA modules. The realization of elements connection (implementation of the developed logical structure into FPGA) is provided by the special interface equipment supplied by FPGA developer.

The test of SHC E&PRP technical condition is performed automatically after power switch-on and continuously during the working process. After the switch-on, the component parts working capacity, operability of input and output circuit, absence of distortions in programs, correctness of data transmission via communication lines are controlled. During the operation, power supply, temperature and smoke level monitoring inside cabinets, absence of program hang-ups, validity of input signals and digital data, proper performance of each channel are permanently and automatically controlled. In case of any failure detection, workstation and MCR gives the corresponding alarm message which form and content allow to quickly and accurately detect the place, time, character and hazard level of the failure. The message is comes with audio signal. Display of unreliable data detected during the input signals diagnosis is accompanied by clearly distinguishable and uniquely understandable marker. The required diagnostic depth (to changeable component parts in each operating stand-alone unit) is provided by built-in diagnostic means.

The input and output signals of SHC E&PRP are shown at Figure 4, place SHC E&PRP in reactor control & protection systems - at Figure 5.

Software has multi-component structure and consists of system and application software.

System software includes operational and supporting software. Operational software contains means, which the application programs call appeal directly. Supporting software (tools) is used for development of application software, debugging and testing of SHC E&PRP and its component parts at the operation location.

The main functions are performed by the complex programmable electronic components (FPGA).

A*pplication software* has a two-level structure. Low-level software provides activity of the functional and communication processors built in blocks of temperature sensors signal input, analog and discrete information input, USB-OPTO interface adapters, functional and set-point processors in the protection signal forming blocks.

At the low-level of application software the following software tools are used:

- FPGA electronic designs performing protection functions;
- Processor software by Texas Instruments company, developed on Assembler programming language;
- Software developed on C programming language for Altera Nios process emulator implemented into FPGA Cyclone logical structure.

The adopted by developers strategy of data processing task distribution among many low-level microcomputers, absence of direct connections between the performed calculation processes, as well as abandoning of program methods for performing of the most complex functions the performance of which is transferred into FPGA, allowed to simplify the structure and to reduce software volume. It resulted in decrease of error possibility which cannot be detected during software verification (and risk of common cause failures which could be caused by such errors).

External appearance of software-hardware complex SHC E&PRP are shown at Figure 6.

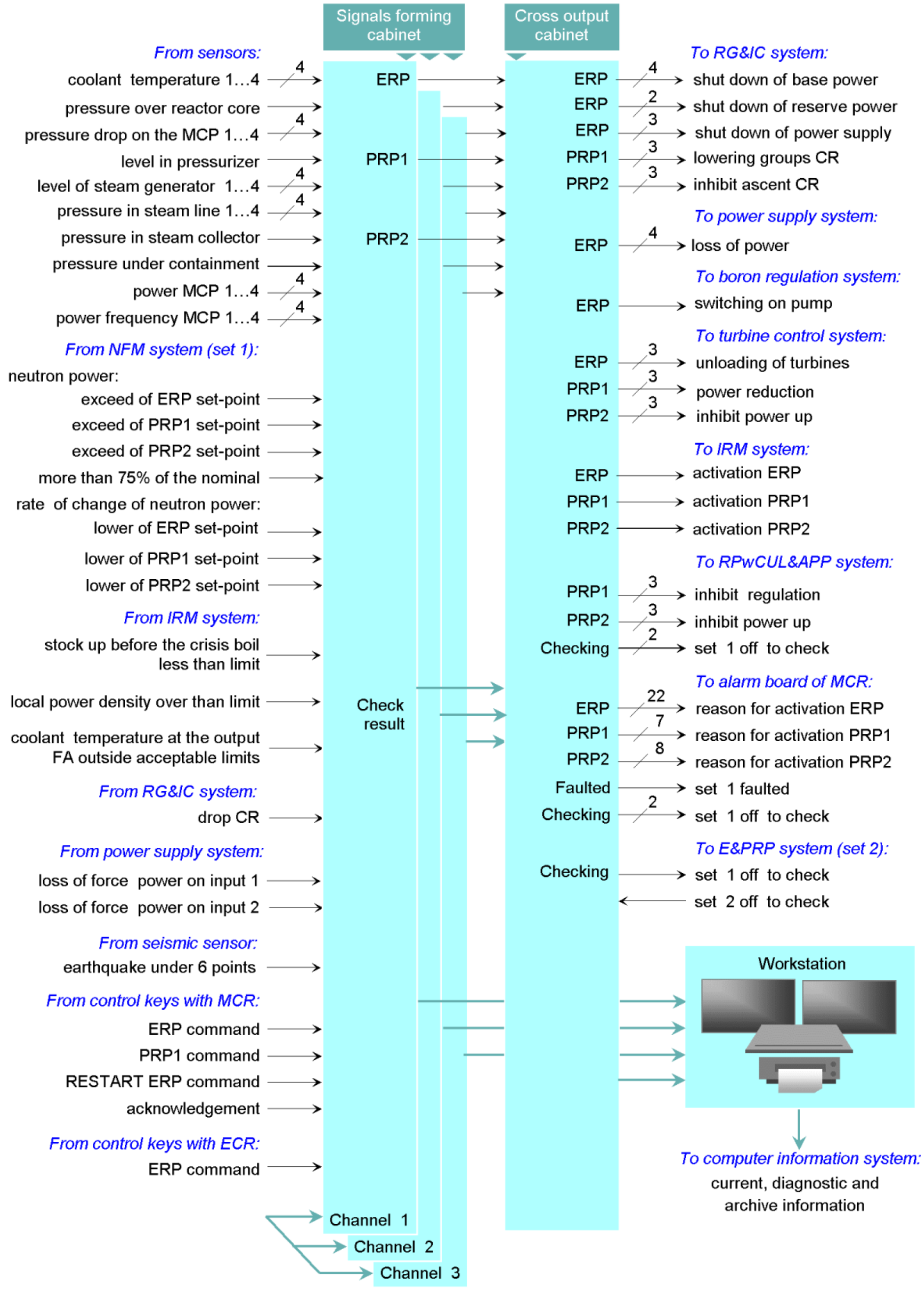
SAFETY ASSURANCE

SHC E&PRP belongs to the elements of safety control systems, that is why all the applied fundamental and technical safety principles regimented for such elements in Ukrainian regulatory documents and international standards are realized in it.

SHC E&PRP functions required for NPP safety assurance are performed in any initiating event and failure of one of the elements which is independent of the initiating event (*single failure principle*). The requirement for survival in any type of failures, as well as in case when the failure of one elements causes failures affected by it, is regarded. The possibility of hidden failure is additionally regarded. SHC E&PRP structure allows to save survival in case of failure of any quantity of elements in one channel of the first and / or second set, as well as in case of several different elements failure in two or three channels in each set.

In SHC E&PRP the *redundancy principle* is observance: each set has the independent protection channels on each of the parameters which characterize limits and / or safety performance conditions. Redundancy is one of the main structural SHC E&PRP features. In the redundant channels of each set the three-step feature based redundancy is applied. Redundancy of primary and secondary

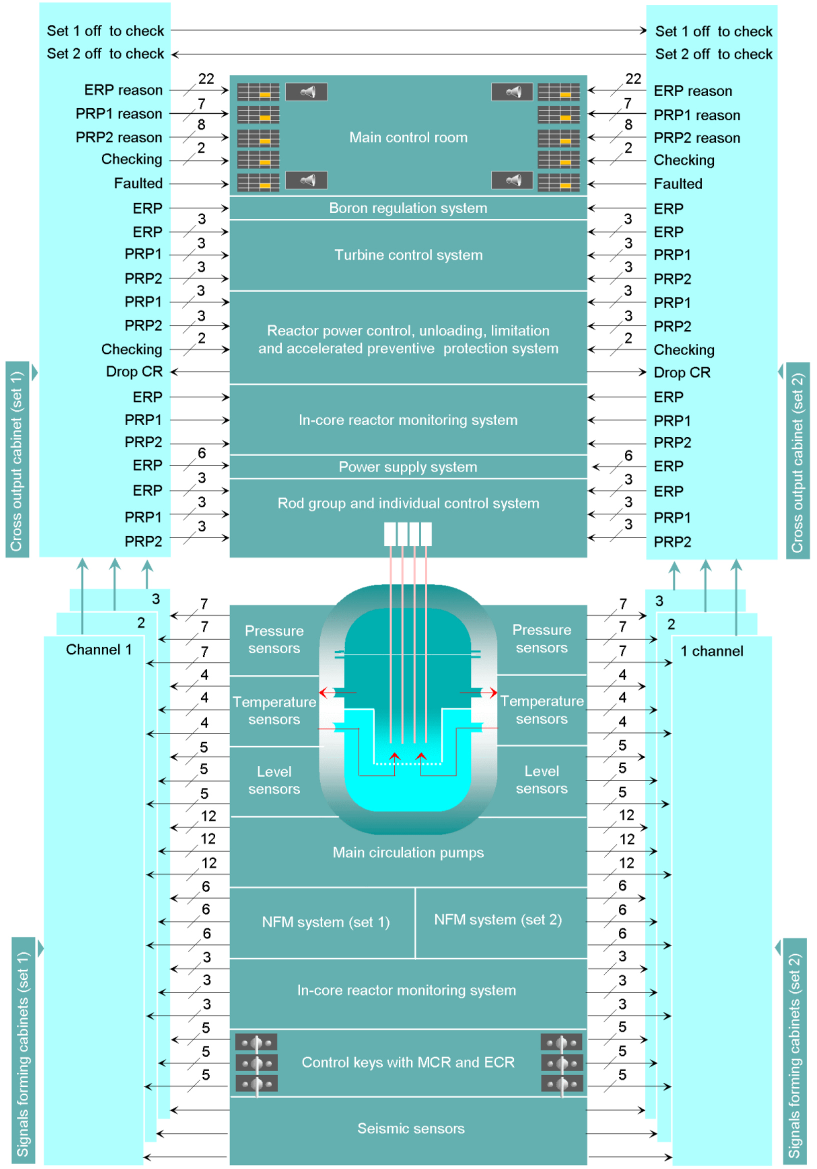
Figure 4. The input and output signals of SHC E&PRP



power source, workstation videomonitors, as well as functional redundancy (data duplication on the workstation videomonitors and inbuilt panel computer monitor, data sending to CIS, etc.) are additionally provided.

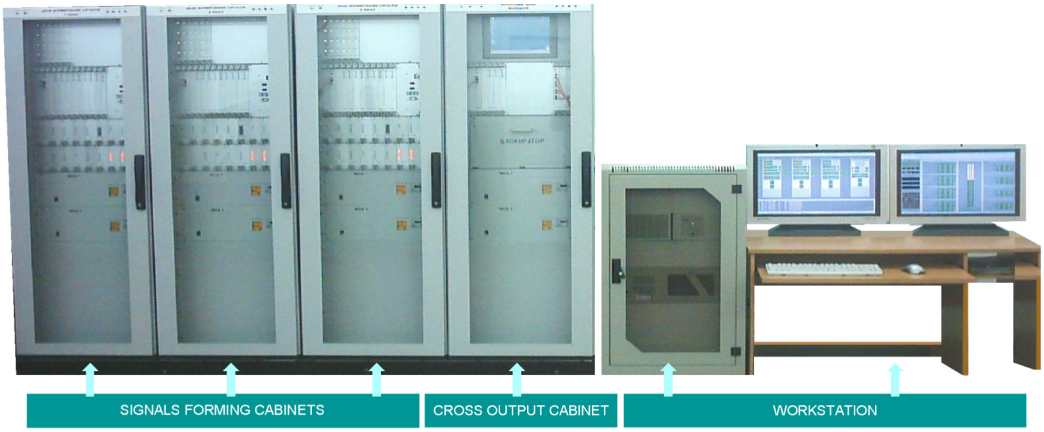
SHC E&PRP saves the ability to perform the functions required to safety assurance in case of failure or removal of one redundant channel or system connected with it (*principle of independence*). For this purpose, the following is provided:

Figure 5. SHC E&PRP in reactor control & protection systems



- Screening and galvanic isolation of input, output and power supply circuits in each channel using optoelectronic components;
- Usage of radial communication structure ("point-to-point") between the channels which provide saving of possibility and correctness of data transmission between the other channels in the case of failure of each one channel;
- Physical separation of the SHC E&PRP redundant channels located in separate cabinets and receiving primary power supply from different sources;
- Usage of fiber-optic communication lines for data transmission between operating stand-alone component parts of SHC E&PRP.

Figure 6. Software-hardware complex SHC E&PRP: external appearance



Operability preservation in case of failure or removal of any sensor and any system related to SHC E&PRP (or such system redundant channel) is provided by application of separate independence input signal sources for each of three redundant channels and organization of separate independence outputs for each protective command sent to redundant channel of the adjacent system.

In SHC E&PRP the *diversity principle* is provided: software and hardware diversity is provided, which is realized due to element base difference used in the first (primary) and second (diverse) set, and eliminates common cause failure caused by possible mistakes during design and / or factory defects of purchased components (as operating experience shows, nowadays they pose one of the most real danger). For this purpose in diverse set are used purchased components of other types and / or received from other manufacturers. The accepted diversity variant has, in comparison with the others, the advantage that in both sets the unity of main system, circuit, and design solutions, external communications and connection methods is saved, that substantially simplifies and reduces cost of design, approbation, manufacture, testing, NPP personnel preparation and performance of the main and diverse sets, at the same time decreasing risk of errors during their maintenance.

In the software development (low-level), including electronic design of FPGA, the subject, design and program diversity is provided. Subject diversity is attained due to that software and electronic design of FPGA, which are used in main and diversity set, is done by different groups of specialists. Design diversity is provided by a range of used instrumental software development tools and means for FPGA logic structure design. In SHC E&PRP development the *preventive and protective common cause failure* means are provided, which include:

- Possible personnel mistakes during operation and maintenance;
- Influence of abnormal natural phenomena (earthquakes, lightning strokes);
- Operation conditions in place of autonomous items location;
- Errors during software development.

In order to prevent common cause failures, the means required to resistance of function performance of operating stand-alone component parts are provided: to temperature, pressure, humidity, mechanical vibrations and shocks (including the ones caused by earthquakes), electromagnetic interference and other factors possible during operation at the NPP, as well as in case of parameters current supply deviation .

Each cabinet is provided with continuous control of primary power supply on both inputs and measuring of secondary power supply source output voltages. Information about primary and secondary power supply are sent to workstation for displaying and archiving. Power disconnecting of power supply on both inputs in at least on cabinet leads to forming of general signal "Set Failure", which is sent to MCR.

Protection of redundant channel failures caused by defects of purchased components and errors during software development (including electronic designs of FPGA logic structure) is provided by diversity principle realization.

SHC E&PRP sets *quality assurance* is guaranteed by system of quality design, product development, manufacture and delivery management at RPP "Radiy" (certificate of conformance with standard ISO, 9001). The current quality management system is certified by International Community of engineering supervision (TÜV NORD GRUPPE). Development, manufacture, testing of the deliverable complete set were held in accordance with quality assurance programs developed by RPC "Radiy" in accordance with ISO, 2000.

Solutions and Recommendations

Information about excess o neutron power values and decrease of power change period in acting now modernized emergency and preventive reactor protection system enter to inputs of SHC E&PRP as discrete signals from neutron flux monitoring systems (from two deliverable complete sets SHC NFMS). This decision accepted in typical design of WWER-1000 unit is not optimal, because it includes the additional devices between neutron-flux detectors to signals forming cabinets of SHC E&PRP, also as cable lines, devices that support SHC NFMS operation, etc.

Recommended to analyze the other decision-elaboration and using in SHC E&PRP special blocks for direct input of signals from neutron-flux detectors. These blocks can be set in signal processing crates, data from them can be process by the same FPGA, as the other input blocks.

FUTURE RESEARCH DIRECTIONS

International experience of nuclear energy usage for peaceful purposes proves the fact that we should not be satisfied with the safety and reliability level that has already been achieved on previously created and used nowadays emergency and preventative unit protection systems, which play the main role in control and monitoring of NPP performance.

The future research trends aimed at improving of emergency and preventive unit protection systems can be: improving of information exchange methods not only between E&PRP system components, but with other control and information unit systems, modernization of human-machine interface, usage of new ways and formats of information protection.

Main future research direction is also upgrading of platforms for SHC E&PRP, what will be used in future. Under the creation of new platforms the appearance of new generations of FPGA and the other electronic components with improving characteristics, also as the introduction of developing now regulations and standard with advanced requirements to I&C functional safety, have to be take in account systems.

CONCLUSION

For the first time at Ukrainian NPPs as a central part of emergency and preventative unit protection were used SHC E&PRP complexes, developed by Ukrainian specialists on base of leading information technologies with usage of world class technical means. During the development the fundamental safety principles were complied (coping of common cause failures, redundancy, independent, diversity, etc.) and requirements of current Ukrainian and International NPP safety regulations and standards. The accepted conception of successive multistep tests provided sufficient depth and validity of the results.

The complexes comply to the fire safety, seismic resistance, electromagnetic compatibility requirements, they are resistant to external effects possible at the operating site, including power circuit noise, ground network noise, signals and command transmission chains noise, communication lines noise, as well as room space noise, where the operating stand-alone items are located.

The inbuilt diagnostic system, independent from the elements engaged in main control and information functions performance, provides automatic technical state test after power supply switch-on and continuous defects detection during the performance (with the depth to interchangeable part), archiving, display and registration of diagnostic messages. The possibility of quick recovery by “hot” change of failed component (without normal operation mode switch-off) is provided.

All SHC E&PRP sets passed the whole licensing cycle and were admitted as complying with the respective requirements of the national and international nuclear safety regulatory documents and used almost at all Ukrainian NPP units.

Successful operation experience (since November 2003) proved the propriety of made technical decisions and SHC E&PRP use perceptiveness for emergency and preventative unit protection systems reconstruction at the NPPs and for new NPPs.

REFERENCES

IAEA. (1999). *Basic safety principles for nuclear power plants.75- INSAG-3, Rev. 1*. Vienna, Austria: IAEA.

IAEA. (2002). NS-G-1.3. *Instrumentation and control systems important to safety in nuclear power plants: IAEA safety guide*. Vienna, Austria: IAEA.

IAEA. (2012). SSR-2/1. *IAEA safety standards*: *Safety of nuclear power plants: Design: Specific safety requirements*. Vienna, Austria: IAEA.

IEC. (2006). IEC 60880. *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.*

IEC. (2009). IEC 61226. *Nuclear power plants — Instrumentation and control systems important for safety — Classification of instrumentation and control functions*.

IEC. (2011). IEC 61513. *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*.

IEEE. (1978). IEEE 338. *IEEE standard criteria for the periodic surveillance testing of nuclear power generating station safety systems*.

ISO. (2000). ISO 9001. *Quality management systems - Requirements*.

KTA. (1985). KTA 3501. *Reactor protection system and monitoring equipment of the safety system*. Cologne, Germany: GRS.

NP. (1997). NP-001-97. *General provisions on the safety of nuclear power plants*. Moscow, Russia: Russian Federal Supervision on Nuclear and Radiation Safety.

NP. (2000). NP 306.5.02/3.035. *Nuclear and radiation safety requirements to instrumentation and control systems important to safety to nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2008a). NP 306.2.141. *General provisions on the safety of nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2008b). NP 306.2.145. *Nuclear safety regulations the reactors nuclear power plants with pressurized water reactors*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NUREG. (2002). NUREG-0800. *US nuclear regulatory commission: Standard review plan: Section 7.0: Instrumentation and control - Overview of review process*.

ADDITIONAL READING

ANSI/IEEE (1987). ANSI/IEEE 352. *Guide for general principles of reliability analysis of nuclear power generating station protection systems*.

Bakhmach, E., Siora, A., Bezsalyi, V., & Yastrebenetsky, M. (2008). Digital systems for reactor control: Design, Experience of operation. *Proceedings of the 16th International Conference on Nuclear Engineering ICONE16*, Orlando, Florida, USA.

KEY TERMS AND DEFINTIONS

Channel: An arrangement of interconnected components within a system that initiates a single output. A channel loses its identity where single output signals are combined with signals from other channels, e.g., from a monitoring channel, or a safety actuation channel.

Diversity: A property related to a group of two or larger number of I&C systems and SHC, which simultaneously and independently from each other perform functions identical for achieved safety purposes, and differ from each other by an operating principle, structure, applied component parts, software and / or other attributes or achieve a target goal in different ways.

Emergency Protection: I&C function, intended for a rapid transfer and a long support of a reactor core in a subcritical state, that is characterized of a value of an effective multiplication factor, less than one, and a lack of a local criticality.

Preventive Protection: I&C function, intended for limitation or decrease of a reactor power to a safety level in case of normal operation violation.

Redundancy: Application of additional means and / or possibilities, redundant in regard to those, which are minimum required for function performance.

Safety Function: A specific purpose that have to be fulfilled for safety assurance.

Standard: A set of mandatory requirements with which compliance is not a legal requirement, but with which failure to comply without valid reason would be negligent.

Chapter 10
Rod Group and Individual Control System

Yuri Rozen
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Alexander Siora
Research and Production Corporation Radiy, Ukraine

ABSTRACT

Chapter 10 considers the Rod Group and Individual Control (RG&IC) system, which is one of the individual I&C systems and a part of the reactor control and protection system. RG&IC is an actuation system, which performs functions initiated by emergency and preventive reactor protection, reactor power control, unloading, limitation and accelerated preventive protection, and remote control rod position commands sent by the power unit personnel. The central part of RG&IC system consists of software-hardware complex SHC RG&IC-R based on the equipment family of the Research and Production Corporation "Radiy" (RADIY PLATFORM – see Chapter 1). The RG&IC system combines functions that belong to A and B categories according to safety impact (IEC, 2009), relates to safety class 2(A) and complies with the fundamental safety principles (IAEA, 1999), requirements that are set forth in international standards (IAEA, 2002, 2012; IEC, 2011), and Ukrainian nuclear safety rules and regulations (NP, 2000, 2008a, 2008b).

INTRODUCTION

Modernization of rod group and individual control (RG&IC) systems at Ukrainian NPPs provides the replacement of out-of-date equipment of the central part with new software-hardware complexes, which are designed basing on positive domestic and foreign experience in compliance with the following main provisions:

- Preservation of the rod group and individual control functional purpose, algorithms, priorities of control functions and performance principles of control rod drives provided by the operational system;
- Preservation of the peripheral equipment (sensors of control rod position and control rod drives) used in the operational system;

DOI: 10.4018/978-1-4666-5133-3.ch010

- Preservation of operational system connections with other power unit I&C-systems: emergency and preventative reactor protection (E&PRP) system; reactor power control, unloading, limitation and accelerated preventive protection (RPwCUL&APP) system; in-core reactor monitoring (IRM) system; computer information system (CIS);
- Preservation or reduction of the existing cable lines;
- Improvement of application properties and operational durability (reliability, maintainability, availability) by using of modern information technologies, new electronic components produced by world leading manufacturers, industrial PCs, diagnostics, etc.;
- Compliance with requirements of nuclear and radiation safety rules and norms, obligatory requirements of any other Ukrainian standards and international standards requirements.

As a technical base of rod group and individual control system modernization on power unit 1 at South-Ukrainian NPP the designed Research and Production Corporation (R&PC) "Radiy" software-hardware complex SHC RG&IC-R was accepted. The use of this complex for modernization of similar systems at the other South-Ukrainian NPP power units is provided.

SHC RG&IC-R is designed for work with the peripheral equipment (control rod drives and sensors of control rod position) of all types used at the Ukrainian NPPs.

All main SHC RG&IC-R functions (input signals transformation, logical operations performance, control algorithms realization, forming of controlling actions on control rod drives) and a range of auxiliary functions (diagnostics, etc.) are realized basing on field programmable gate arrays (FPGA), which electronic designs are developed and implemented by RPC "Radiy", while in software-hardware complexes from other providers such functions are performed by microprocessor controllers and/or industrial PCs under system and application software. The use of FPGA provides high flexibility (adjustment to realization of different I&C functions) comparable to the computing hardware programmable means capabilities, and, at the same time, good predictability of behavior and testability of SHC RG&IC-R main functions, typical for the devices with unconditional logic ("hard-wired technology"). It decreases the risk of common cause failures, which can be caused by the errors during FPGA electronic design development, in comparison with the risk of possible hidden errors during computing operations programming. Besides, parallel (simultaneous) way of FPGA functions realization allowed to increase SHC RG&IC-R speed.

BACKGROUND

Chapter 8 provided information on way of neutron power control by moving of the absorbing rods in the reactor core and a short description of the system, which performs functions of rod group and individual control being a part of reactor control and protection system at the Ukrainian NPPs. In this Chapter the detailed information on the purpose, performed functions, technical specifications, composition, structure and software of the SHC RG&IC-R complex within the modernized RG&IC system at South-Ukrainian NPP unit 1 is provided, along with the assurance of its functional safety.

Information on control rod drives and sensors of control rod position is provided in this Chapter in quantity required for understanding of SHC RG&IC-R performance; detailed description, specifications and experience of using of such peripheral equipment is given in the book Nikituk, 2004.

Characteristics of RG&IC system and SHC RG&IC-R, provided in this Chapter, are the example of specific realization of the general properties of safety important I&C systems and their components, provided in Chapter 3, which take into account the purpose, categories of the performed functions and safety class of SHC RG&IC-R.

PURPOSE

During the power unit operation the reactivity change in the nuclear reactor takes place, which is caused by the continuous fuel burn, slagging and poisoning, which influence reactor thermal power and speed of its change. In order to maintain normal power unit exploitation in the operational modes this change must be compensated. The slow reactivity change is compensated by the change of liquid/fluid poison (boric acid) concentration in the coolant, which is usually clean demineralized water, at the same time, serving as a neutron absorber (Boron regulation system). Fast change of reactivity is performed by the mechanical control rods movement with a solid neutron absorbers – absorbing material made of boron carbide and titanic dysprosium powder put into a enclosure vessel (Gorochov, 2004).

In the WWER-1000 reactors control rod (CR) is a construction of 18 vertical thin absorbing elements, which are located at some distance from one another, and hard-secured at the top. Each control rod can move in special guiding channel inside the fuel assembly. Power unit 1 of South-Ukrainian NPP has 49 CR, on other Ukrainian power units with WWER-1000 reactors the number of CR was increased to 61. Each control rod is identified by two coordinates – numbers of horizontal and vertical row of CR, which are represented on the fuel assembly's positioning map in the reactor core (core map – see Figure 1).

CR of each group is located symmetrically to the center of reactor core and at proximately equal distance from it. Closer to the center than all others, are located control rods of the sixth group, then – fifth and tenth; the most distant are CR, which form third, fourth and ninth groups.

Each CR has its own controlled electromechanical step-motor, with the help of, which it can move vertically in the reactor core independently of the other CR ("individual control") or synchronically with a few other CR, which form one of ten fixed control rods groups ("group control").

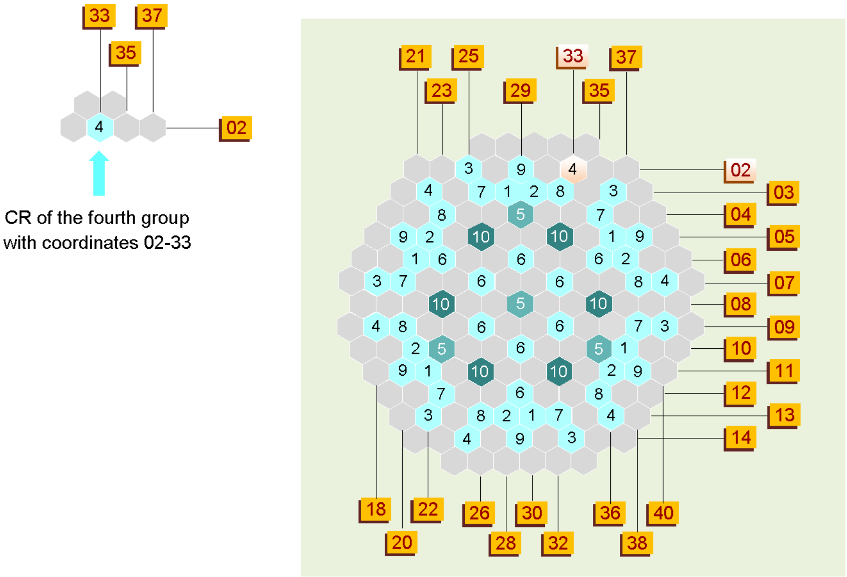
In individual control the selection of one of CR and control of its movement is performed via operating personnel commands. Group control provides simultaneous lift (or lowering) of all CR, which are the parts of the corresponding group, however, the selection and movement control of any group (except the fifth one) can be performed via operating personnel commands, and also automatically. Movement control of the fifth group intended for aligning of power density axial distribution (vertically) in the reactor core and for xenon oscillation suppression (see Gorochov, 2004) is performed only via the operating personnel commands.

While downwards movement (lowering) of control rod, neutron absorber, which is in it, is put into the, in this case, multiplication factor decreases and, as well as neutron reactor power; while upwards movement (lift) of control rod reactor power increases.

Control rods move in the reactor core vertically to the fuel assembly's (for WWER-1000 reactors operational range is 3500 mm). The limits of operational range are usually interpreted as a position of the virtual upper limit switch (ULS) and lower limit switch (LLS): CR movement is stopped by the sensor of CR position signals corresponding to the positions of ULS and LLS. All performance range between ULS and LLS is figuratively divided on 10 equal sections, which borders are defined by the sensor of CR position signals.

In the reactor subcritical state all CR are in lower limit switch position. In order to bring the reactor into critical state and into minimal controlled power level a successive lift of CR groups (except the fifth one) into the upper core

Figure 1. Plan of disposition of fuel assemblies in the core (core map)



is performed – in the ULS position. The lift is performed in design order with the nominal speed (20 mm/sec). To prevent core heat-up caused by too fast power increase and the limited ability of coolant to cope with big quantity of generated heat, each CR group is lifted in such way, that after its movement on the defined distance (350 mm for WWER-1000 reactors) sending of controlling actions to all control rod drives of the group stops and renews no sooner than after 60 sec. The last (usually – tenth) CR group is lifted in the position providing the optimal power density control for power operation. Sensors of control rod position allow performing continuous monitoring of positions of all CR vertically in the core. For WWER-1000 reactors is provided the following:

- Automatic movement control of CR groups in a strict design order (the fifth group is excluded from the design order);
- Manual movement control of CR group (besides the fifth one) or one CR at the operator’s option;
- Manual movement control of the fifth CR group;
- Dragging of CR, which did not reach ULS or LLS positions after the whole group was stopped;
- Alignment of CR positions within the group;
- Drop of all CR or previously selected CR group on lower hard support;
- Lift by operator’s command and setting in the LLS position all CR, which are on lower hard support after the fall.

Automatic control mode is realized by commands “Boost” (B↑), “Decrease” (D↓), “Preventive reactor protection” (PRP1), “Reactor power unloading” (RPwU) from the adjacent systems.

In order to decrease power density variation vertically in the core while moving CR groups in the strict design order the main (work) and auxiliary CR groups are defined. While upwards movement the main group is that for, which the following requirements are provided: the inserted in it CR are above lower limit switch, and all groups with higher sequence numbers included into design order — in LLS position (this requirement is not applied to group 10 as a group with higher sequence number does not exist).If all groups are in LLS position a group with a sequence number 1 is selected as the main group.

In other cases, the main group is previously defined CR group (while upwards movement) or a group with the closest lower sequence number (while downwards movement).

The condition for simultaneous movement of the main and auxiliary groups is a location of the main group near upper or lower performance range limit in the positions, which are figuratively called upper intermediate switch (UIS) and lower intermediate switch (LIS) position. The same as for limit switches, the used names mean not the physical elements, but CR positions, for, which the performance of the functions below is provided. It is considered that the group reached a set position after this position was reached by any four (while upwards movement) or three (while downwards movement) CR, which are in the group of six control rods (groups 1-4, 7-10 in Figure 1), or by any CR in a group, which consists of nine control rods (group 6 in Figure 1).

After the group, which moves upwards reached UIS position, the closest auxiliary CR group with higher sequence number starts moving with it. In case of stop of the main group after it reached ULS position, or after the auxiliary group reached LIS position, the main group sequence number automatically increases by one (auxiliary group becomes main group). For example, lift of groups from the position when all they are in lower limit switch is performed in the following design order:

- The main group with a sequence number 1 starts moving upwards;
- Upon reaching of upper intermediate switch position by, at least, four any CR of the main group, the auxiliary group with a sequence number 2 starts moving upwards;
- Each CR of the main group, which reached upper limit switch position, spots by the signal from its sensor of control rod position and stays in this position;
- Upon reaching of upper limit switch by four of main group CR (or upon reaching of lower intermediate switch position by four auxiliary groups CR) the main group becomes group 2. Following the lift of new main group the other CR of group 1 reach upper limit switch position according to the set algorithms.

The mentioned actions repeat for all groups (except the fifth one not included into the design order) successively in increasing order of indices until four CR of group 10 reach the position shown in Figure 1, or until exit this mode by operator’s initiative.

During power operation group with a sequence number 10 is in the operative position, and the rest groups – in ULS position. If power decrease required, CR lowering is performed in the following design order:

- A group with a sequence number 10, which starts moving downwards is selected as the main;
- Upon reaching of lower intermediate switch position by, at least, three any main group CR, the auxiliary group with a sequence number 9 starts moving downwards;
- Each CR of the main group, which reached lower limit switch position stops by the signal of its sensor of control rod position and stays in this position;
- Upon reaching of lower limit switch position by three of main group CR (or upon reaching of upper intermediate switch position by three auxiliary group CR) the main group becomes group with number 9. Following the lowering of new main group, the delayed group 10 CR reach lower limit switch position according to the set algorithm.

The mentioned actions continue for all groups included into the design order consequently in the decreasing order of indices until 3 CR of group 1 reach lower limit switch position or until they exit this mode by the operator's initiative. CR group, which are already in lower limit switch position, for example, dropped earlier by the command of accelerated preventive protection, is excluded from the design order. If such drop takes place during downwards movement of the groups, the main group stays the previously selected CR group; if the group, which was the main at the moment was dropped, a new main group becomes a group with the closest lower sequence number.

Control commands to control rod drives are formed in rod group and individual control (RG&IC) system. Automatic control by the command PRP1 from the adjacent E&PRP system or by the command of RPwU from the adjacent RPwCUL&APP system provides moving of the groups downwards in the design order starting from the group, which has the highest sequence number and is not in lower limit switch position.

During the action of PRP1 and RPwU the commands of automatic control B↑ and D↓ are blocked from RPwCUL&APP system and from group control key. Blocking of automatic control commands can also be performed by the operator with the help of the key on remote control in the main control room (MCR) premises. In case of absence of PRP1 and RPwU commands and unlocked commands of automatic control, the latter initiate (by command B↑) or lowering (by command D↓) influence to main and auxiliary groups, as well as the group, which provide CR "dragging" (if required).

CR group manual control mode provides group control of the position of any CR group selected by the operator or individual control of the position of any selected CR.

Selection of CR group is performed by setting up the switcher on remote control in one of the positions (from 1 to 10), which corresponds to the group number control over, which will be performed via group control key, for example, can be selected a group dropped by the signal from accelerated preventive protection for its lift to the design level. While working in the automatic mode for manual control can be selected a group, which is auxiliary (or a group, in which CR "dragging" is provided). For example, if some CR delayed from the positions of other CR of the group, operator chooses this group and drags such CR to ULS (or LLS) positions holding the group control key in B↑ (or D↓ accordingly) direction. Commands from the group control key influence only the selected CR group. Selection of the group for manual control does not influence the conditions and sequence of group movement by the automatic control commands PRP1, RPwU, B↑ or D↓. In case of simultaneous commands entry the higher priority have PRP1, RPwU and D↓ commands in comparison with B↑.

Selection of CR for individual control is performed on remote control located in MCR, for example, by input of this CR coordinates (see Figure 1) or by pushing the respective button on a core map, which shows the location of all CR. Movement direction (lift or dropping) is set by "Boost" (B↑) and "Decrease" (D↓) commands from individual control key in the MCR. Movement of the selected CR does not influence the position of other control rods and does not depend on their movement in the group the selected CR to.

Individual control mode has the following features:

- The selected control rod retains the ability to move along with the other CR of the respective group in group control mode (retaining the above mentioned priorities concerning movement directing);
- If the selected CR to the main or auxiliary group, which is at the moment moving by the automatic control command B↑ or D↓, individual control of this CR is possible only after the automatic control commands blocking;
- In case of simultaneous influence on CR of the commands initiated by individual

control key, group control key and/or automatic control key, the downwards movement command (PRP1, RPwU, D↓) is of high priority.

Manual control movement mode of the fifth CR group is used for alignment of power density axial distribution in reactor core in stationary and transient modes on the neutron power level within the range 30% to 100% of the nominal. CR of the fifth group are inserted into the core if the influence of main (working) and auxiliary groups on power density axial distribution is not sufficient. Control is initiated by "Boost" (B↑) and "Decrease" (D↓) commands from the separate control key. Featuring of a separate control key allows the operator to move CR of the fifth group not influencing the other groups and independently of their position. Operator moves the whole group (and "drags" delayed CR of the group), holding the control key until all CR of the fifth group reach the end position (ULS or LLS). As the fifth group is not included into the design order, PRP1, RPwU, D↓ and B↑ commands do not act on it.

CR "drags" mode is meant for moving of the delayed CR, which did not reach ULS (while lift) or LLS (while lowering) into the end position after the group was no longer the main one.

Dragging is performed only during movement in the respective direction of the next CR group, which is set as the main. Downwards movement command for dragging CR, which did not reach LLS has the priority over lift commands of the same CR in case of individual control.

CR positions alignment mode is realized if the position of, at least, one CR in the main (work) group deviates from the middle position of CR in this group for more than ± 40 mm. In this case operator automatically receives the signal about the need of alignment, information on position of all CR in work group is displayed and CR, which positions must be aligned with other are indicated.

Drop of previously selected CR group or all CR on lower hard supports provides fast change of reactor neutron power by the accelerated preventive protection command from RPwCUL&APP system or emergency reactor shutdown by the emergency reactor protection command from E&PRP system. Drop is realized by the basic, reserve and power supply cut off for all control rod drives of respective CR group previously selected for accelerated preventive protection realization, or for all control rod drives, and in the result the respective CR drop by gravity on lower hard supports. Fall of CR group leads to fast reactor power decrease (accelerated unloading), fall of all CR – to emergency reactor shutdown (chain reaction termination and reactor subcritical state transition).

For all work modes of rod group and individual control system the priorities of control functions performing described in the following section.

FUNCTIONS

Along with adjacent systems, power unit operating personnel and technological equipment, RG&IC system is engaged in reactivity control (IAEA, 2002), which provides:

- Automatic regulation of reactor power and/or power change by operator's commands;
- Automatic power decrease (reactor removal of load) in case of set design limits or normal performance requirements violation;
- Reactor shutdown (transition of reactor core into subcritical state).
- Basing on the main system purpose, software-hardware complex SHC RG&IC-R must perform main (control, information) and auxiliary functions.

Control Functions

- In case of absence of commands from adjacent I&C systems or from the operating personnel: Retaining of all CR in the end or any intermediate positions (including cases of power interruption during the time set by the design);
- By emergency reactor protection (ERP) command, received from any of two SHC E&PRP sets: Disconnecting of power supply of all control rod drives, which cause CR drop under their own weight into lowermost position (on lower hard supports), (then – drop of CR into the core);
- By accelerated preventive reactor protection (RAPP) command, received from SHC RPwCUL&APP: Disconnecting of power supply of CR driving mechanisms of one (previously selected) group, which causes drop of all CR of the group into the core;
- During preventive reactor protection (PRP1) command action, received from any of two SHC E&PRP sets, or reactor power unloading (RPwU) command, received from SHC RPwCUL&APP: Forming and sending control signals to control rod CR drives, which provide lowering of CR groups with the nominal speed in the design order starting from the last removed group;
- During action of preventative preventive reactor protection (PRP2) command, received from any of two SHC E&PRP system sets: Forbidding of all commands performing, which initiate CR lift;
- By the commands of automatic regulation received from SHC RPwCUL&APP: Forming and sending to control rod CR drives of control signals, which provide lift (by B↑ command) or lowering (by D↓ command) with the nominal speed simultaneously all CR of one group selected by the operator with the help of switcher on remote control and monitoring panel in MCR or moving of the groups one by one in the design order;
- By the operator's initiative (by B↑ or D↓ command from the group control key on remote control and monitoring panel in MCR): Forming and sending control signals to control rod CR drives, which provide lift or lowering with the nominal speed simultaneously of all CR of one group selected by the operator with the help of switcher on the same remote control panel, or moving groups one by one in the design order;
- By the operator's command B↑ or D↓ from the control key on the remote control in MCR: Forming and sending control signals to control rod CR drives, which provide lift or lowering with the nominal speed simultaneously of all CR of the fifth group;
- By the operator's initiative (by the command B↑ or D↓ from individual control key on the control and monitoring panel in MCR): Forming and sending to control rod CR drives of the control signals, which provide lift or lowering simultaneously with the nominal speed of any CR or several CR (up to six) selected by the operator with the help of buttons embedded in the core map on the same control panel;
- By the operator's command from the key on control and monitoring panel in MCR: Forming and sending control signals to control rod CR drives, which provide successive lift (by groups in order of priority) of the CR, which upon performance start or after drop by ERP or RAPP command are on lower hard support, and their stop at the

CR movement lower performance range value (in lower limit switch position).

Distribution of CR by groups, sequence of groups movement and priorities of control functions performing in case of simultaneous performing of several functions at the SHC RG&IC-R input are defined by rod group and individual control algorithms, which are set in the reactor design. SHC RG&IC-R realizes priorities of control functions performance used at the Ukrainian power units with WWER-1000 reactors:

- **Emergency Reactor Protection:** In relation to the other functions: when ERP commands is received, it is performed immediately, after that performance of other control functions is suspended and can be renewed only after ERP command cancellation at the SHC RG&IC-R input;
- **Accelerated Preventive Protection:** In relation to the other control functions except emergency reactor protection: when RAPP command is received, it is performed immediately, after that reactor power unloading (RPwU) command must be performed;
- **Preventive Reactor Protection PRP1:** In relation to the other control functions except ERP and RAPP: during PRP1 command performance of B↑ and D↓ automatic regulation and manual control commands is blocked (RPwU command performs the same actions as PRP1);
- **Preventive Reactor Protection PRP2:** In relation to any actions, which prescriptive upward movement of any groups or separate CR: during PRP2 command performance of B↑ automatic regulation and manual control commands is blocked;
- **Downward Movement of Any Groups or Separate CR:** In relation to any actions, which prescriptive their upward movement.

In case of simultaneous entry of commands from group control key and fifth group control key at the SHC RG&IC-R input, only group control command is performed.

Information Functions

- Displaying: coordinates of CR selected by the operator for individual control; number of group selected for manual group control; number of main (work) group and CR auxiliary group while their moving in the design order;
- Indication of movement direction (lift or lowering) of the moving CR or CR group;
- Monitoring of all CR position within the operating cycle stroke range (between LLS and ULS) and identification of two end and ten intermediate position of each CR;
- Monitoring and displaying of the precise (with 1% discretion) vertical position: selected by the operator CR or selected CR group; main (work) CR group while moving in the design order; each CR group (intermediate position); all CR in one (any one selected by the operator) group;
- Monitoring of vertical mismatch of all CR in each group and sending of alarm message led by sound signal in cases when position of, at least, one CR deviates for more than ± 40 mm of the middle position of the group, which this CR to constituent;
- Detection of fall of, at least, one (any) CR into the core and sending of the signal, which initiates forming of PRP2 command, to the first and second SHC E&PRP sets;
- Forming and sending to the in-core reactor monitoring system (IRMS) of data on the precise vertical positions of all CR;
- Forming and sending to power unit computer information system of messages with data on: group control commands, initiated by the operator and / or received from the adjacent systems; coordinates of control

rod selected for individual control; number of the main and auxiliary groups moved in the design order.

Additional Functions

- After power switch-on and during operation: Automatic diagnosis, archiving and continuous displaying of diagnostic information on SHC RG&IC-R technical condition, its parts, interconnecting lines, control rod drives and sensors of control rod position, detection of failure places or defects appearance, sending of generalized signal on SHC RG&IC-R failure in CIS and to the indicator in MCR;
- During operation and testing (drop of CR): Automatic monitoring, archiving and displaying (upon personnel's request) of each CR parameters, which characterize:
  - Delay of CR drop start (from sending of the respective command to SHC RG&IC-R input or disconnecting of power supply until CR get from upper limit switch position;
  - Full falling time of CR from upper limit switch position to lower hard support and transmission time of each section of operating stroke range;
  - Delay of CR leaving of lower limit switch: From sending of B↑ command to SHC RG&IC-R input until the moving CR reach the low limit of operating stroke range (LLS position);
  - Transmission time of the moving CR for each section of operating stroke range while upwards (by B↑ command) and downwards (by D↓ command) movement, the whole transmission time of CR within the operating stroke range between LLS and ULS;
- During testing: Forming of protocols for each CR and general protocol for all CR with pointing:
  - Electromagnet current in control rod drives (with dispersion indices);
  - Average CR movement speed for upwards and downwards movement;
  - Distance, passed CR from ULS to LLS, between from LLS and ULS and of each section of operating stroke range;
  - Height of each CR movement section of operating range;
  - Quantity of CR double strokes and drops;
- Archiving of data on SHC RG&IC-R and CR performance in operating modes and during testing (general duration and quantity of double strokes within traveling operating stroke range, quantity of CR drops by protection commands, given by the operating personnel manual control commands, etc.);
- Synchronization of SHC RG&IC-R current time with NPP universal time system data.

Functions, which provide emergency reactor protection belong to A category, CR retention functions, accelerated preventive protection, preventive reactor protection, reactor power unloading, reactor power automatic regulator and power change by the operator's commands— to B category (see Chapter 2).

CHARACTERISTICS

Rod group and individual control system combine fulfilling of safety functions with safety related functions (functions of normal operation, in terms of Ukrainian regulation NP, 2008,a) and related to safety class 2(A) (in Ukrainian documents), which coordinate, according to IEC, 2011, to safety class

1 (see Chapter 2). The same is classification of the central part of this system - software-hardware complex SHC RG&IC-R. Important to safety operating stand-alone component parts of SHC RG&IC-R related:

- Components which take part in emergency reactor protection – to safety class 2(A);
- Components which take part in accelerated preventive protection, preventive reactor protection PRP1, reactor power unloading, reactor power automatic regulator, also as function of group control by operator commands, – to safety class 3(B) (safety class 2 according to IEC, 2011);
- Components which take part in preventive reactor protection PRP2 and individual control (if they are not ranged in more high safety classes), - to safety class 3(C) (safety class 3 according to IEC, 2011).

Operating stand-alone component parts SHC RG&IC-R destined (see Chapter 3):

- For operating in the rooms of electrical equipment's and software-hardware complexes normally access area (group of operation conditions E2.2), except devices, installed in the rooms with air condition (MCR, ECR, etc.), which belong to E2.3 group of operation conditions;
- For setting on the building constructions in case of absence of closely–spaced sources of mechanical influences (group of location condition P1.1), except devices of manual input and displaying, set on supporting constructions (panels or boards), which belong to P.1.2 group of location condition;
- For operating in rooms with electromagnetic environment of medium hardness in compliance with NP,2000.

SHC RG&IC-R fulfills all specified functions after mechanical influence, which imitate project earthquake (6 point), and functions emergency reactor protection and monitoring of rod control position after mechanical influence, which imitate maximum calculation earthquake (7 point). Parameters of imitated influences (required response spectrum) is given in Chapter 3.

Every deliverable complete set supplied from three inter-redundant safe power sources by three-phase alternating current with 380 / 220 V. Operating stand-alone component parts supplied by direct current with 24 V power from two independent inter-redundant sources (located in secondary power cabinets, including in deliverable set), each of them receives energy from NPP auxiliary power, or from two independent feeders of single-phase alternating current network 220 V via no-break power supply.

Primary force power supply of RC drives is performed from two power sections by three-phase alternating current with 380 V and from redundant direct current source with 110 V (accumulator battery with charging device). Each drive is supplied from the respective power control channel: main – by alternating current with 144 V or 250 V (related from type of RC drive), redundant – direct current 110 V. For transformation of alternating current primary power three-phase 380 / 144 V or 380 / 250 V transformers are used. Allowable long-term drifts of the alternating current power are from minus 15% to plus 10%, frequency – from minus 2% to plus 2% of the nominal value. Power interruptions (time - to 20 ms) during communication from one source to other, short drift of power from minus 30% to plus 25% during 2 s and frequency from minus 5% during 10 s don't lead to failures or necessity of restart or reload.

SHC RG&IC-R are immune to electromagnetic external influencing factors (electromagnetic disturbances), which can influence from power ports, input and output ports, communication ports, ground ports, from outer surface of device enclosure. List of types of disturbance, parameters of test influences, simulating disturbances of each type and places of their application, also as criteria of estimation coordinate with international standards devoted Electromagnetic compatibility (EMC) and identical to them Ukrainian state standards (see Chapter 3 and Rozen, 2007; Rozen, 2008).

Reliability measures define fulfilling reliability of control and information functions according criteria described in Chapter 3 (Table 1).

Mean Time to Restoration (MTTR) for devices recoverable on operating site and fulfilling control functions – no more 1 hour, fulfilling information functions - no more 2 hours. Component parts, which include in operating standalone devices, permit replacement without power shutdown and without own adjustment and adjustment of the other connected component parts. Mean life (durability measure) of deliverable complete set are not less than 30 years.

CONSTRUCTION PRINCIPLES

Composition of deliverable complete set SHC RG&IC-R is shown at Table 2, structure of a software-hardware complex - at Figure 2 (for basic control functions) and Figure 3 (for basic information and additional functions).

For data exchange between SHC RG&IC-R component parts (devices) electrical discrete signals and / or) digital messages sent via fiber-optic communication lines are used. Data on CR position are sent to sensors of CR position, which are in MCR and ECR, in form of electrical analog direct current signals. Messages from workstation are sent to In-core reactor monitoring system and unit computer information system via duplicated optical communication channel using TCP / IP protocol.

The deliverable set includes electrical and optical cables, which connect all operating standalone component parts of SHC RG&IC-R, and also optical cables and related equipment (commutation switches, adapter units) for data transfer to IRMS and CIS.

Table 1. Reliability measures of SHC RG&IC-R

Function	Measures		
	availability	**failure flow parameter**	**mean time between failures**
Execution of ERP commands	0.99999	$1,0 \bullet 10^{-5}$ 1 / h	-
Execution of RAPP commands	0.99999	$2,0 \bullet 10^{-5}$ 1 / h	-
Execution of PRP1 commands	0.99997	$3,0 \bullet 10^{-5}$ 1 / h	-
Execution of PRP2 commands	0.99997	$3,0 \bullet 10^{-5}$ 1 / h	-
Execution of RPwAR (B↑, D↓) commands	0.999985	$1,0 \bullet 10^{-5}$ 1 / h	-
Execution of operator commands	0.999985	$1,0 \bullet 10^{-5}$ 1 / h	-
Information to MCR panel	0.999	$1,0 \bullet 10^{-4}$ 1 / h	-
Display of operator directives	0.99996	$2,0 \bullet 10^{-5}$ 1 / h	-
Display of CR positions	-	-	$1.0 \bullet 10^{5}$ h
Output information about CR position to IRMS	-	-	$2.5 \bullet 10^{4}$ h
Output digital messages to CIS	-	-	$2.0 \bullet 10^{4}$ h

Table 2. Composition of deliverable complete set SHC RG&IC-R

Name	Amount	Safety class	Category of earthquake resistance	Group of operation conditions	Group of location conditions
Signals forming cabinet	3	2(A)	I	E.2.2	P.1.1
CR position cabinet	4	2(A)	I	E.2.2	P.1.1
Power control cabinet	16	2(A)	I	E.2.2	P.1.1
Secondary power cabinet	4	2(A)	I	E.2.2	P.1.1
Control and monitoring panel	1	3(B)	II	E.2.3	P.1.2
Workstation:	1	3(B)	II	E.2.3	P.1.1
LCD video display unit	2	3(B)	II	E.2.3	P.1.2
Laser printer	1	4	III	E.2.3	P.1.2
Industrial keyboard	1	3(C)	II	E.2.3	P.1.2
Indication device	2	2(A)	I	E.2.3	P.1.2
Block of time synchronization	1	4	–	E.2.2	P.1.2
Set of cables	1	–	–	–	–
Set of service equipment	1	–	–	–	–

Deliverable sets are oriented at specific type control rod drives and sensors; however, there is a possibility to transfer to another type of a CR drive and / or sensor of control rod position by reconfiguring of deliverable set available means. Reconfiguring does not require modification or change of the deliverable set equipment and is provided by respective technical means, program codes and installation instructions from SHC compositions.

Signal forming cabinets perform emergency and accelerated preventive reactor protection, as well as group and individual CR control. Three identical cabinets form three independent channels, which reserve each other. Each channel (cabinet) receives:

Figure 2. Structure of software-hardware complex SHC RG&IC-R for basic control functions

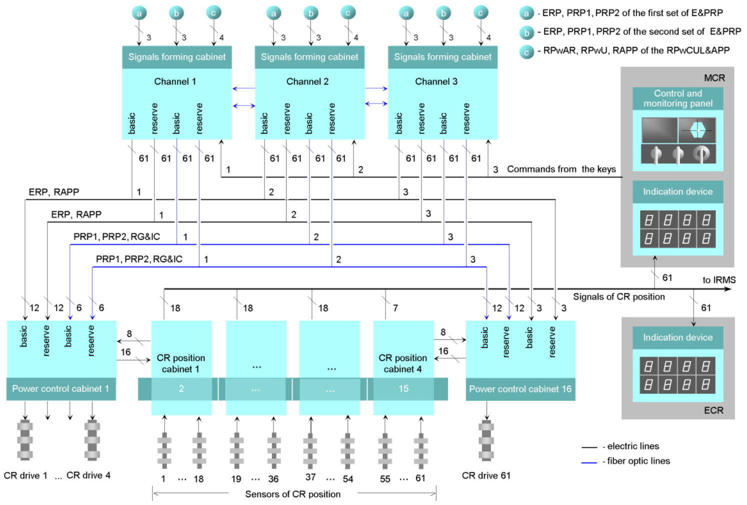
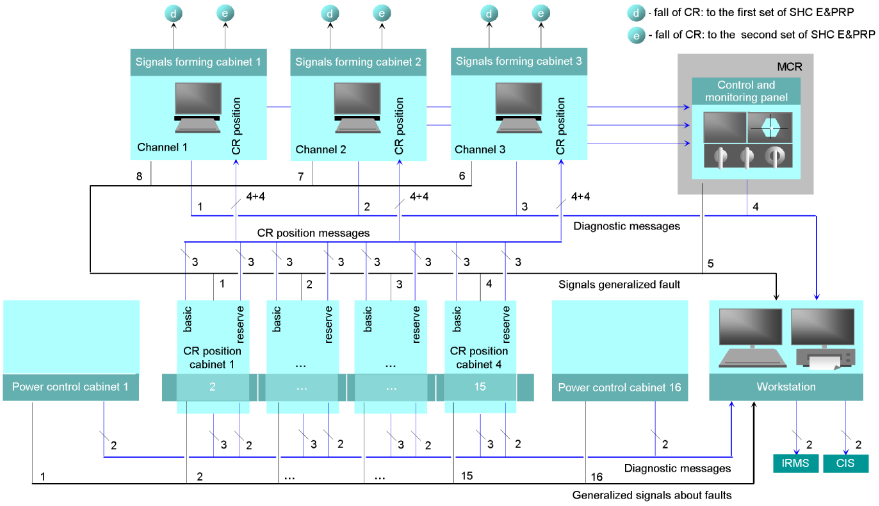


Figure 3. Structure of software-hardware complex SHC RG&IC-R for basic information and additional functions

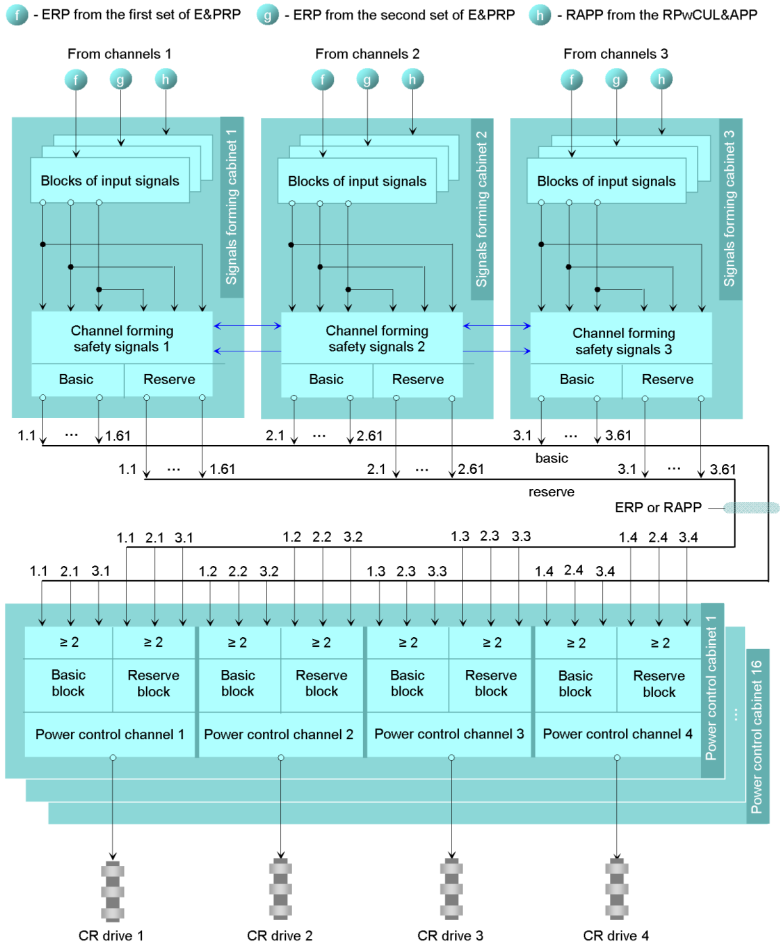

d - fall of CR: to the first set of SHC E&PRP
e - fall of CR: to the second set of SHC E&PRP
Signals forming cabinet 1
Signals forming cabinet 2
Signals forming cabinet 3
Channel 1
Channel 2
Channel 3
CR position
MCR
Control and monitoring panel
4+4
CR position messages
Diagnostic messages
Signals generalized fault
basic
reserve
CR position cabinet 1
CR position cabinet 4
Power control cabinet 1
Power control cabinet 16
Workstation
IRMS
CIS
Diagnostic messages
Generalized signals about faults

- Commands of emergency and preventative protection (ERP, PRP1, PRP2) from one of three independent channels of the first and second SHC E&PRP-R set;
- Commands of reactor power control, unloading, limitation and accelerated preventive protection (RPwAR, RPwU, RAPP) from one of three SHC RPwCUL&APP independent channels;
- Commands and directions of manual (individual and group) control initiated by the operator via monitoring and control panel in MCR (all elements of panel have separate independent outputs for connection to each channel);
- Data about vertical CR position in the core, CR falls, duration of falling.
- Galvanic isolation of input circuits and supply circuits, which receive each commands, is provided.

Each signal forming cabinet sends digital data on condition of its inputs in two other channels via fiber-optic communication lines, receives from them similar data, performs data logical processing, and in case of mismatching detection - forms error signal and corrects unreliable input information (also taking into account rules of interpretation of possible malfunctions while digital message transferring between channels, set for different input signals. For example, absence of data from any channel is interpreted as presence in this channel of PRP1, PRP2, RPw U command, absence of RPwAR command, etc.

On emergency reactor protection commands received from the first and second SHC E&PRP set, each signal forming cabinet forms control signals and sends them to each power control cabinet, where they initiate disconnecting of power supply on direct and alternating current of CR drives, which are controlled by this power control cabinet. The same actions are activated by RAPP signals which are formed in signal forming cabinet by command of accelerated preventive reactor protection, received from SHC RPwCUL&APP, but they are transmitted only to power control cabinets, which control the group of CR drives previously selected for this command realization (group selection is performed in signal forming cabinet). Scheme of realization of commands of emergency and accelerated preventive protection is shown on Figure 4.

Figure 4. Implementation of emergency and accelerated preventive reactor protection commands

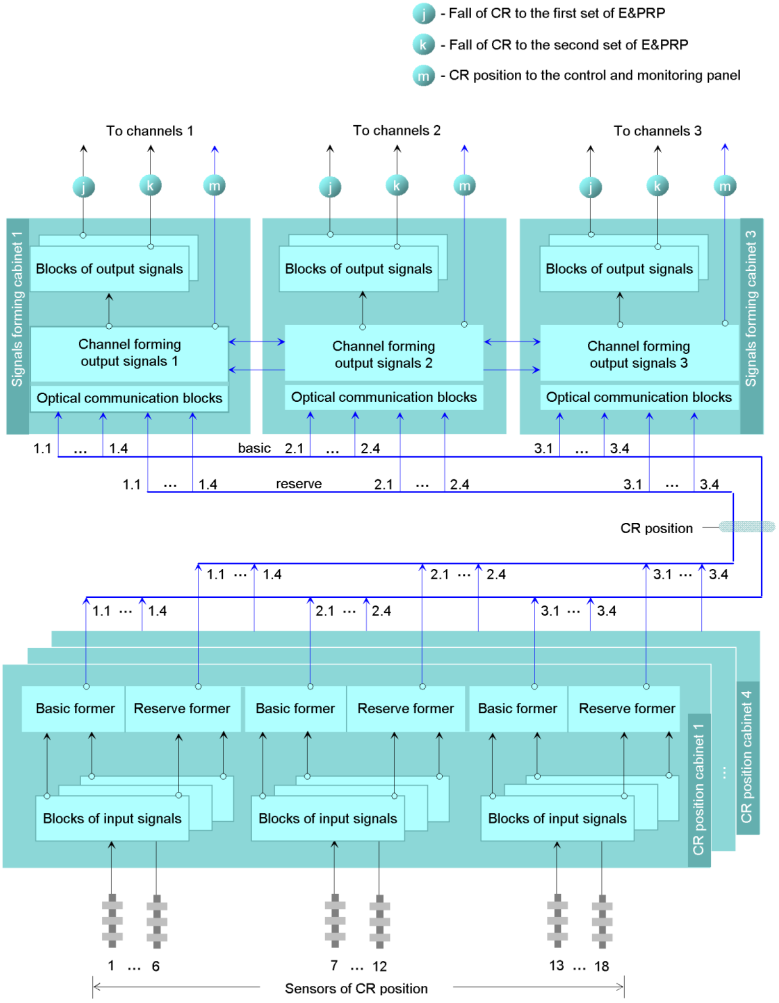


Each signal forming cabinet has base and reserve protection signals forming channels. Their outputs are connected by separate wires to the base and reserve blocks of each power control channel in all power control cabinets. Actuation of power control channel (forming and delivery of control signal, which activate power off of appropriate CR drive) take place, if on input of basic block this channel logical element “≥2” commands from ERP or RAPP activate simultaneously from two or all three channel forming safety signals. If basic block is in down state, which is detected by diagnostic means, power control channel activation realizes by reserve block of this channel with the same conditions.

Forming and displaying of data on CR position is shown in Figure 5.

Digital messages from CR position cabinet are sent via fiber-optical communication lines, which form the main and redundant control buses, to channels of output signals forming on the first, second and third signal forming cabinet. Each channel transmits the received digital messages via fiber-optical communication lines to the same channels in two other signal forming cabinet, receives from them similar messages and compares them with data received via main and redundant control buses. In case of data mismatching output signal forming channel corrects unreliable input information forming error signal. In case of re-

Figure 5. Forming and displaying data about control rods positions

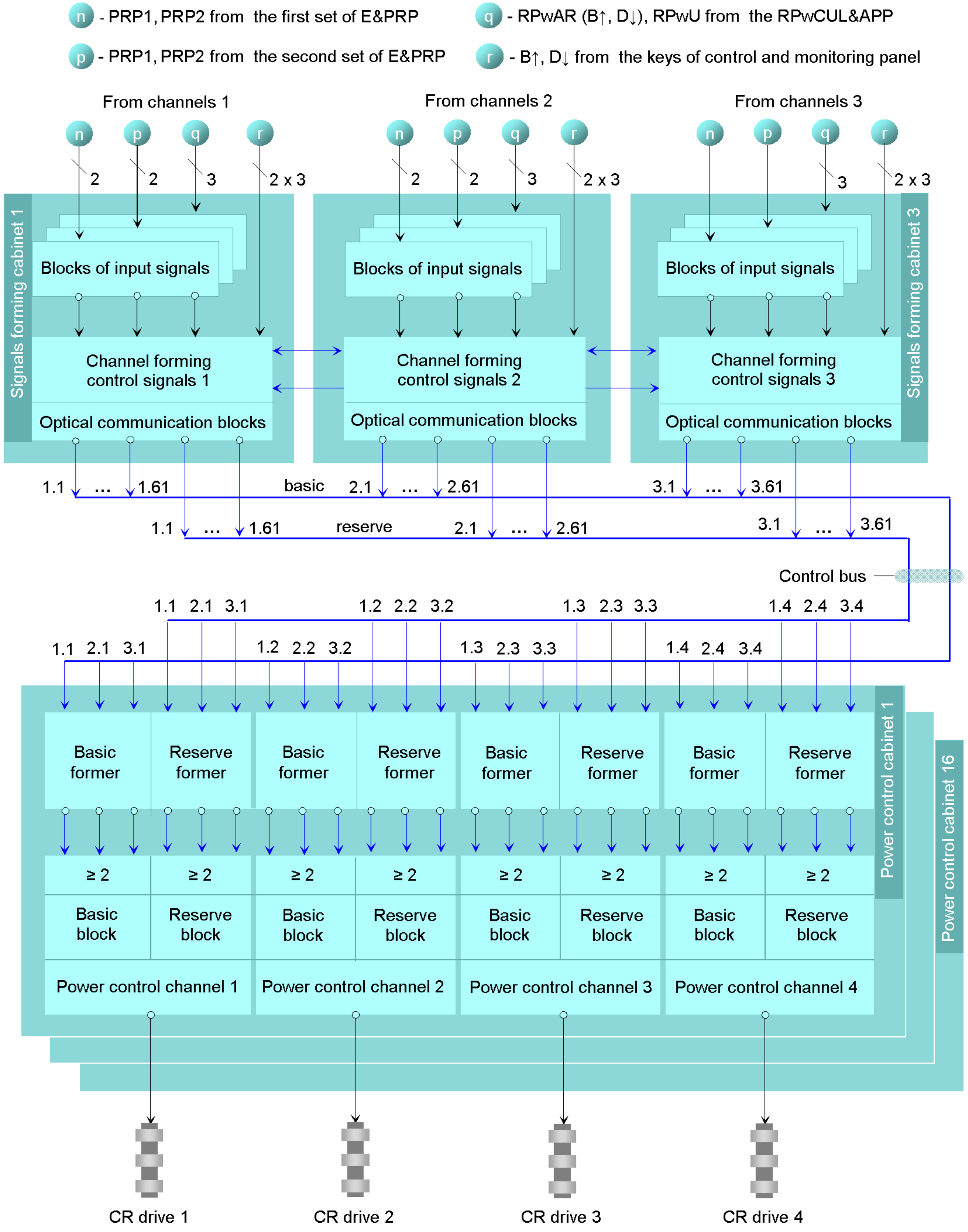

j - Fall of CR to the first set of E&PRP
k - Fall of CR to the second set of E&PRP
m - CR position to the control and monitoring panel
To channels 1
To channels 2
To channels 3
Signals forming cabinet 1
Signals forming cabinet 3
Blocks of output signals
Channel forming output signals 1
Channel forming output signals 2
Channel forming output signals 3
Optical communication blocks
1.1 … 1.4
basic 2.1 … 2.4
3.1 … 3.4
reserve
CR position
Basic former
Reserve former
Blocks of input signals
CR position cabinet 1
CR position cabinet 4
1 … 6
7 … 12
13 … 18
Sensors of CR position

ceiving information on CR drop, as well as if due to malfunction any group or separate CR starts upward movement without command B↑, signal forming cabinet forms and sends to the respective channels of the first and second set of SHC E&PRP signals initiating PRP-2 preventative protection actuation. Data on CR drop are fixed in position control channel of control rod position cabinet; after pressing button "PRP-2 PICKUP" on control and monitoring panel command is sent to signal forming cabinet and from them to all position control channels initiating reset of previously fixed information and termination of signal forming, which initiate actuation of PRP-2 (in Figure 5 is not shown).

On base of data received from CR position cabinet in every output signal forming channels are continuously defined: vertical position of each CR group in the core; number of main (work) and auxiliary group while moving in the design order; reaching by the moving group of upper or lower (limit and intermediate) switch.

Group and individual control commands are realized according scheme on Figure 6.

Figure 6. Commands of group and individual control implementing



During PRP-1 preventative protection command or command of reactor unloading (RPwU) every signal forming cabinet forms signals, which initiate downwards movement of CR and transmits them via fiber-optical lines (marked in Figure 6 as control bus) to power control cabinets, which control main group drives. After the main group reached position of lower intermediate switcher signal forming cabinet starts transmission of signals, which initiate movement of CR also to the power control forming cabinets, which control auxiliary group drives. Transmission of signals on main CR group movement is stopped as it reaches position of lower limit switcher.

In the same way forming and sending of signals on upward (downward) CR movement by the command of automatic control B↑ (D↓) from SHC RPwCUL&APP or from group control key on control and monitoring panel (if group selection switch is set in position, which corresponds moving of groups in design order). If switch is set on a specific CR group, upwards (downwards) movement signals are transmitted via control bus only to the power control cabinets, which control the selected group drives. By command B↑ (D↓) from individual control key on control and monitoring panel every signal forming cabinet forms upwards (downwards) movement signal and sends it by control bus to power control channel, which controls the selected CR group drive.

Forming and transmission of signals in performed in accordance with commands control priorities. During PRP-2 command from the first or second SHC E&PRP set, as well as in case of influence on key set on MCP, which controls opening of valve pure condensate input into the first circuit, forming and sending of any signals on CR upwards movement is blocked. If commands received from different sources require simultaneous movement of two CR groups, the highest priority has preventive protection command PRP-1, lower –RPwU and manual control command D↓, next – manual control command B↑, the lowest priority have commands B↑ and D↓ from the RPwCUL&APP system. To bring all CR, which did not reach upper (while lift) or lower (while lowering) end switch to the end position dragging algorithm is performed for the rest CR after the respective group is no longer the main one.

Each signal forming cabinet forms and sends to control and monitoring panel data on vertical position of all CR, misalignment of CR in each group and alarm message in case of excess of allowable misalignment (± 40 mm) in, at least, one group. With the help of SFC diagnostic blocks of signal forming cabinet continuous automatic monitoring of components and connection lines technical condition is performed. Diagnostic message on the monitoring results and data on the received commands from first and second set E&PRP system, RPwCUL&APP system, control and monitoring panel are sent to workstation via fiber-optic lines (Figure 3). Generalized signal about faults is sent to workstation via separate lines from every signals forming cabinet, where failure any component parts or defect interconnecting lines are detected.

Panel PC with touch-screen display and duplicating keyboard is used for setting (change) of group components and selection of CR group. On the computer display snapshots with data on control mode, received commands, coordinates of selected CR, number of the moving group in case of manual control, etc., can be displayed.

CR position cabinets are intended for work with linear or stepwise position sensors.

Linear position sensor consists of coil block, case, cover and magnetic shunt. Coil block includes mechanically-connected single-wound coils: seven base ones placed at the same distance from one another and two reserve: one is placed between the first and the second, the other – between the second and the third base coils. In order to isolate the first circuit, coil block is placed in solid sealed case in form of variable section pipe made of non-magnetic steel. The whole case along with coil block is inside of the moving bar, to which fastens control rod.

Magnetic shunt in form of magnetic soft steel pipe is embedded inside the bar (in its upper part) and covers sensor case along with coil block. Shunt length is a bit more than half of the core height. Coils and shunt are placed to each other in such way that when CR is positioned on lower hard support shunt covers ("overlaps") one of the base coils (lower one), and when lift in lower limit switch position – two. Then the quantity of coils covered by shunt increases by one while upwards movement of CR on each 350 mm. In CR position in the middle of lower and upper limit switch shunt covers all seven main coils. Further lift leads to decrease by one of quantity of coils covered by shunt while upwards movement of CR on each 350 mm up to upper limit switch position in, which shunt does not cover any of the coils.

Cover protects coil outputs and places of soldered connections on electrical connector sensor from environmental influence (under containment). The base coils are series-connected and supplied by alternating current. In case of coil coverage by magnetic shunt its inductance rises, with that total resistance of series-connected base coils (and sensor output signal - voltage decrease from flowing current) depend on quantity of oils covered by magnetic shunt. It allows to define the CR position within the borders of each of 10 sections, which all the CR movement range is divided into, as well as CR position on upper and lower limit switches (accuracy to ± 20 mm at the end and ± 30 mm at the intermediate sections). Reserve coils allow to find out CR fall in case of base group coils failure.

Signal from each sensor of CR position is transformed into staircase (multilevel) signal, which information parameter is direct current, which identify number of section within the borders of which CR is at the moment, as well as CR position on upper and lower limit switch. Two indication devices are used for imaging with single digit indicators gathered in 10 groups in accordance with CR allocation in groups. This means of displayed has name *rough* indication of CR position.

For operators' convenience, which got used to decimal system, each section is divided into 10 fixed stages (35 mm each), which makes 1% of whole upwards CR movement in the core. In such a way, movement of CR on each stage is performed in the result of one or two steps, movement on one section – 175 steps (nominal step of CR drive equal to 20 mm). CR position within each section is determined by count of quantity of steps made by the CR drive after the border of respective section was crossed. In such a way, CR position displayed of two digital characters, the first of, which corresponds to section number, the second – to stage number within the section where CR is at the moment. Such means of displayed has name *precise* position indication. On the control and monitoring panel are three blocks with two-digit indicators for precise indication of middle positions of main and additional CR groups and position CR, controlled manually.

Another type of linear sensors of control rod position differ from the described sensor only in quantity, connection and placement of inductance coils (reserve coils are not provided). Six coils are divided in two groups (upper and lower), each of them is formed by three series-connected coils. Coils supply is performed from CR position cabinet in form of sum of alternating (100 ± 1 mA, 120 ± 1.2 Hz) and direct (40 ± 0.4 mA) current components. Output signal is formed as components of alternating and direct voltage, which are defined by complex resistance of the upper and lower coil groups, dependable of shunt position. On the results of its processing, discrete signals are formed for rough CR position indication (section number, position CR on upper and lower limit switch). Precise CR position indication is determined by the section number and quantity of steps made by the CR drive on each section.

Stepwise sensor allows to define control rod position with 20 mm discretion, i.e. within one drive step, that is why for precise indication the count of drive steps in not required. Such possibility was reached due to usage of shunt, covering 9 inductance coils of the sensor in, which magnetic and non-magnetic segments of different length alternate in such way, that if shunt position changes on one step, at least one of 9 coils changes its inductance (Nikituk, 2004). It allows to receive a unique code combination (9 coils with separated inputs can form $2^9 = 512$ different combinations, 191 of which are used, also within working range between upper and lower limit switch – 175 code combinations).

Coils are placed on 100 mm distance from one another, fastened by non-magnetic remote patches and are embedded inside the case from magnetic soft steel, filled by nitrogen. Coil wound is made of heatproof wire on core of magnetically soft steel, coil finishes are out of sensor case, through wall tube. Coils of each sensor are supplied from CR position cabinet of stabilized alternating current (200 mA, 250 Hz). Usage of stepping sensor provides a possibility to diagnosis CR drive (detect skip of steps and slippage), and in case of falling of control rod – to determine duration of CR passing over each section of the core.

Each of three CR position cabinets has 18 independent CR position monitoring channels, fourth cabinet has 7 channels. Each channel:

- Sets current of a specified form and frequency required for sensor performance; receives signals from sensor; defines rough CR position and send direct current continuous signals to indication devices in MCR and ECR;
- Receives impulses from the adjacent channel in power control cabinet, each of them corresponds to upwards or downwards drive movement on one step; counts quantity of steps made by the drive inside the respective section of rod operating; defined precise CR position and sends continuous direct current signal, which represents the precise CR position;
- Forms and sends signals initiating drive stop in case the control rod reached position of lower or upper limit switch into adjacent channel in power control cabinet;
- Receives signal of electromagnet CR drive disconnecting of power supply from adjacent channel in power control cabinet; identify control rod falling (on transmission time from section 2 to lower limit switch, if it is shorter than 4 s); switches on light-emitting diode on the front panel; defines CR transmission time of each core section and general duration of falling;
- Sends to each signal forming cabinet (via base and reserve fiber-optical lines) data on rough and precise CR, electromagnets disconnecting of power supply, CR falling and duration of falling.

Each CR position cabinet performs continuous automatic monitoring over technical condition of its component parts, CR position sensors and communication lines (resistance and inductance of coils, isolation resistance, absence of disconnection and short circuits). Diagnostic messages on test results are sent to workstation (along with data on CR falling duration). Generalized signal about faults is sent to workstation via separate line.

Power control cabinets are intended for direct control of CR drives. One cabinet has four power control channels; each of them controls one drive, performing the following functions:

- Receiving of electrical signals from each signals forming cabinet initiated by emergency reactor protection and accelerated preventive protection commands ERP or RAPP via basic and reserve buses (see Figure 4); logical processing of the received signals in basic and reserve blocks by "two of three" condition; relieve of power supply voltage by alternating and direct current (disconnecting of power supply of electromagnet drives, which causes CR fall) in case of receiving of control signals from, at least, two signals forming cabinets;

- Receiving of digital messages from each of three signals forming cabinet via basic and reserve control buses (see Figure 6); logical processing of the received data (control commands) in basic and reserve blocks; forming and sending to CR drive electromagnets of impulse sequence (cyclograms), which initiate CR movement in case of receiving of commands from two or three signals forming cabinet; forming and sending of CR holding current in case of absence of control signals from, at least, two signals forming cabinet, as well as by drive stop signal received from the adjacent channel in CR position cabinet;
- Automatic switching to reserve input of power supply by direct current for CR holding in case of losing of alternating current power supply or force control circuit failure (in case of simultaneous current decrease of locking and fixing electromagnets to 50% of the nominal holding current);
- Forming and sending of impulses while each CR movement on one step upwards or downwards and while disconnecting of power supply of drive electromagnets, which is caused (separately) by ERP, RAPP command and actuation of automatic power supply switcher to the adjacent channel in CR position cabinet.

Power control channel has automatic switch-off of basic block outputs in case of reserve block performance, and renewal of basic block performance in case of control return to it. Both blocks are equal, however, one of them is supplied by rectified current from basic power supply source, the other is supplied by direct current from reserve source (accumulator battery). Both blocks outputs are parallel-connected to CR drive electromagnet winding (commutator is not required for switching from the basic block to reserve). While performance from the reserve source drives controllability is preserved. The possibility of in-line electromagnets current change is provided (within the range from 100% to 200% of the nominal values).

Embedded diagnostic equipment performs continuous automatic monitoring over power control cabinet component parts technical condition, electromagnets and communication lines condition (resistance and inductance of coils, insulation resistance, absence of disconnection and short circuits). Diagnostic messages on are sent to workstation via diagnostic and archiving bus. Generalized signal about faults is sent to workstation via separate line.

Monitoring and Control Panel has:

- Switcher to 11 fixed positions, with the help of which one of ten CR groups is selected for manual control, or mode is set, which in case of manual control groups move one by one in a strict design order;
- Switcher to 4 fixed positions with the help of which one of CR groups (number 8, 9 or 10) is selected as the main for automatic power regulation, or mode is set, which by the automatic regulation command (B↑ or D↓) groups move one by one in a strict design order;
- Buttons without mechanic locking for selection of CR, which is selected for individual control (buttons are set on reactor core map- see Figure 1; indication is performed by button after its pushing and lightning map symbol of selected CR);
- Keys on three positions: for selected CR group control (or groups in a strict design order); for control of the fifth group, which

is not included to design order; for control of one selected CR. Upwards movement command (B↑) is sent in case of holding of key in right position, downwards movement command (D↓) – in left position. After lowering key is set in intermediate (fixed) position, with that the command is cancelled;

- Button without locking for exit of the preventative protection mode, initiated in SHC E&PRP by fall CR signal. Button lightning turns on simultaneously with start of fall CR signal sending and turns off after the button is pushed;
- Switcher on 2 fixed positions for putting SHC RG&IC-R from working mode to automatic test mode (test scheduling and procedure, which are supported in automatic test mode, correspond to the specified above).

On monitoring and control panel the following data are displayed: number and direction of CR main (working) group movement (in case of design order group movement the auxiliary group number is shown); vertical position of working group; coordinates of CR, selected for individual control, its vertical position and movement direction. On built-in panel computer, embedded in monitoring and control panel, this information is represented in more details (in a digital form, in form of histograms, mnemonic images, explaining descriptions and notes). By operator's initiative additional data can be displayed: vertical position of all groups and all CR in any group; coordinates of CR, which the middle group position is defined; deviation of each CR position from the middle. In case of deviation of, at least, one CR for more than ± 40 mm of the middle group position alarm message is sent.

B↑ and D↓ commands are sent to signal forming cabinets via separate independent electrical lines. Other information is sent and received in form of digital messages via fiber-optical communication lines, which connect monitoring and control panel to each signal forming cabinet.

Embedded diagnostic equipment performs continuous automatic monitoring of component parts technical condition. Test results are displayed on embedded monitor and transferred to workstation.

Indication devices on MCR and ECR displayed the position of each CR in two limit positions and ten intermediate sections of control rod working stroke. One-digit indicators are placed in 10 assemblies each of them to one CR group; quantity of indicators corresponds to CR quantity in the respective group. Data on position of each CR are sent in form of continuous unified direct current signal (4-20 mA) via separate electrical line, which connects indication device and the respective channel in CR position cabinet. Information signal parameter (direct current) is transformed into discrete signals code combination and displayed in form of digital symbol on indicator, which to this CR.

Workstation, made on base of Hewlett-Packard industrial computer components, performs:

- Receiving of fault signals and diagnostic messages on SHC RG&IC-R component parts technical condition, communication lines, control keys, CR drives, sensors of control rod positions;
- Continuous automatic monitoring of own component parts technical condition (self-diagnosis);
- Processing of received data and results of self-diagnosis, archiving, displayed of current and archived information on industrial monitors; sending of diagnostic messages to CIS and IRMS;
- Sound alarm in case of failure detection, displayed of alarm messages on industrial monitors; forming and sending of generalized signal about faults to CIS and IRMS and to MCR.

Workstation receives from signals forming cabinets, CR position cabinets, power control cabinets data on received and sent commands (signals), current positions of all CR, as well as test results (middle current of each electromagnet, quantity of steps from lower hard support to lower and upper limit switches, and on each section of operating stroke, each section transmission time and total CR movement time in performance mode and in CR falling). The received data are archived and displayed on the monitors. Data on commands (signals) are sent to CIS.

Human-machine interface, which provides interaction of SHC RG&IC-R with unit operational personnel, is supported by manual control commands and operator's instructions input means, signaling and data displaying. To manual control and operator's instructions input means belong keys and buttons on monitoring and control panel. Signaling means include panel "Fault" in MCR, lightning elements of keys and buttons on monitoring and control panel, sound devices and workstation. Data displaying means include indication devices in MCR and ECR, panel computers, indication elements on monitoring and control panel.

Interaction with personnel, realized maintenance of SHC RG&IC-R is provided by: data display means of operating stand-alone component parts, set on their front panels; panel computers of signal forming cabinets; two monitors, industrial keyboard and laser printer of workstation.

Monitoring and control panel is equipped with panel computer with 12" color LED-monitor. All graphical symbols are easily read from 1.5 m distance in illumination typical for MCR. The displayed information is arranged in form of fragments, which are displayed on monitor by the operator's choice. Several fragments (windows) can be displayed on the monitor simultaneously and show, for example, the following:

- Vertical middle position of any selected CR group, deviation of separate CR from the middle position, number of maximum deviated CR, actual and maximum permissible deviation;
- Vertical middle position of all CR groups with pointing of the group, selected for manual control, regulation group, as well as main and auxiliary groups while moving in a strict design order;
- Places on reactor core map of all CR within the group selected for manual control, regulation group, main and auxiliary groups while moving in a strict design order;
- Number of CR group controlled manually, vertical middle position and movement direction;
- Place on reactor core map, coordinates, vertical position and direction of CR movement, selected for individual control;
- Full data on CR, selected for individual control (including duration of its last fail by the ERP or RAPP command);
- Data on monitoring and control panel technical condition, received during diagnosis.

CR vertical position is displayed in digital and quasi-analog form (vertical histograms). Data on technical conditions are displayed in form of topological diagram, which elements are monitoring and control panel replacement component parts. Failed component parts are highlighted by color change and flickering and are transferred on even glowing after alarm message positive acknowledgement by the operator. In case the position of, at least, one CR deviates from the middle position of the moving group for more than ± 40 mm, and in case of generalized fault detection during diagnosis, respective alarm message is displayed on monitor, followed by sound signal.

Workstation is equipped with two 24" color LED-monitors. The displayed information is arranged in form of fragments, which show:

- SHC RG&IC-R technical condition in general and technical condition of all operating stand-alone component parts;
- Information on failure, detected during diagnosis;
- Data on CR fallings (number and coordinates of CR, date, time and duration of falling, start and end CR position);
- Total quantity of steps made by each CR and quantity of steps on each core section;
- CR drives test results.

Data on SHC RG&IC-R technical condition are displayed in form of topological diagram, which elements are operating stand-alone component parts. Failed component parts are highlighted by color change and flickering and are transferred on even glowing the same as in monitoring and control panel. Data on CR falling duration are shown in form of table. Test results are represented in form of chronological list with indication of failure, data and time of their detection and failure recovery. In case of new failure detection sound signal is switched on and respective alarm message is displayed on the monitor.

One video frame on the monitor can contain several fragments, for example, which show SHC RG&IC-R technical condition in general and selected by the operator component parts, data on CR falling duration, etc. The fragment displayed data on SHC RG&IC-R technical condition are displayed on the monitor all the time, other fragments – by the personnel's initiative.

Video frame have hierarchical structure built by "general-to-specific" principle. Call of any video frame is performed with the help of monitor symbols (pictograms) and keyboard or manipulator.

Components. In SHC RG&IC-R were used as element base highly reliable chips, capacitors, diodes, connectors, resistors, varistors, resettable fuses and other electronic components from the leading world manufacturers - Samsung Group, Motorola Inc., Royal Philips Electronics and others. For realization of control algorithms field programmable gate arrays (FPGA), manufactured by Altera Corporation, were used. Usage of FPGA allowed to lessen the quantity of operating stand-alone component parts, provide structure simplicity and efficiency of SHC RG&IC-R and to simplify routine maintenance.

Along with electronic components, in SHC RG&IC-R are used commercial of the shelf (COTS) industrial devices such as panel computers and embedded industrial monitors from Advantech Co., desktop monitors Samsung Group, servers and network commutators Hewlett-Packard Co., uninterruptable power supplies from GE Digital Energy, laser printers from different manufacturers and others.

SHC RG&IC fragment is shown in Figure 7.

SHC RG&IC software has two-level structure.

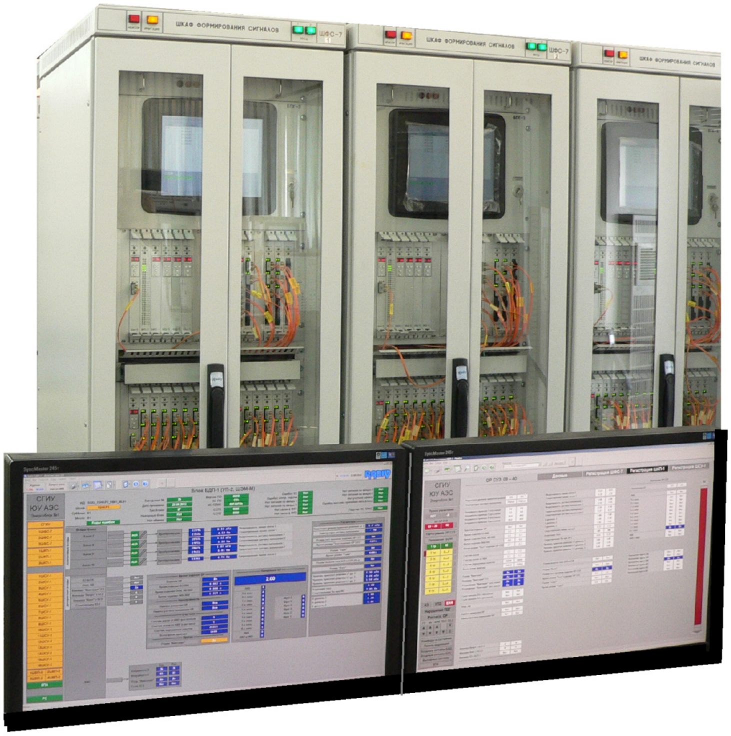
Lower level software, which provides realization of group and individual control algorithms, is developed within FPGA logical structure electronic design. Coding is done in C programming language for functioning in environment Nios processor emulator, implemented in FPGA logical structure. The functions of lower level software:

- Validation of input message;
- Mapping signals, received from linear or stepwise sensor of control rod position;
- Realization of prescribed algorithms of group and individual control;
- Mutual monitoring of three redundancies channels, restoration of corrupted information, bumpless channels switch-on after checks.

Lower level software designed in compliance with requirements, which were set with regard to software, performing functions of categories A.

Upper level software performs informational, auxiliary and service functions: data archiving and displayed; defining of CR falling duration by the command of emergency or accelerated preventive protection in performance mode and during testing (carrying out of CR drop); technical condition

Figure 7. Software-hardware complex rod group and individual control system (fragment)



automatic monitoring and fault diagnostic of SHC E&PRP, adjacent equipment and communication lines, etc. The principal feature of SHC E&PRP upper level software is in the fact that a considerable amount of current and diagnostic information is spread among sets differently servers.

Upper level software designed in compliance with requirements, which were set with regard to software, performing functions of categories B and C. In this software principles of structural and modular programming are implemented. Workstation software works on licensed Microsoft Windows XP Professional Edition operational system, and panel computers software installed in signals forming cabinets – on licensed Microsoft Windows CE 5.0 operational system. Upper level software is developed in C++ programming language. Microsoft Visual C++ integrated development environment, which is a part of Microsoft Visual Studio.NET set, was used as a tool. Microsoft Foundation Classes class library version 7.0 was used during the development.

SAFETY ASSURANCE

With regard to the performed functions and their significance for SHC E&PRP safety on the whole and its components, which are directly engaged in emergency reactor shutdown, belong to safety class 2(A), other components are elements of normal performance and belong to safety classes 3(B), 3(C) or 4. Information about safety classes and categories of earthquake resistance of SHC E&PRP components is shown in Table 2.

In SHC E&PRP new solutions relating to structure, ways of control algorithms realization, circuits engineering, elements base were applied. Safety principles provided by Ukrainian regulatory documents (NP, 2000; NP, 2008,a) and recommended in International standards (IAEA, 2000; IAEA, 2002; IEC, 2011) were realized, that provide reliability, quality, stability and independence of performed functions.

Reliability of functions performance is provided by fulfilling the requirements to prevention and protection of common cause failures, following of single failure principle, reservation and diversity principles, provided personnel error preventive measures, protection from unauthorized access, embedded technical diagnostic means.

Requirements to *prevention and protection of common cause failures* take into account limiting conditions for operation at places of each operating stand-alone component parts (device), influence of abnormal nature influences, personnel error during performance and maintenance, errors during software development, etc. Means directed toward common cause failures prevention and protection are foreseen and realized, correspond to nuclear and radiation safety actual norms and regulations, provided by Ukrainian and international regulatory documents, and minimize possibility of occurrence of causes, which could call such failures.

Requirement to *single failure principle observance*, regimented in SHC E&PRP documents, is provided during development and check-up during deliverable complete set validation. Single failure influence on group and individual control function performance is limited by only one CR.

For observance of *reservation principle* in SHC E&PRP are provided the following:

- Triplicate redundancy with voter of signals forming cabinets (see Figure 2) and duplicated of channels forming safety signals in each signals forming cabinet and power control channels in each power control cabinet (see Figure 4);
    - ◦ Duplicated of signals transmission lines of emergency and accelerated preventive protection from each signals forming cabinet to all power control channels (see Figure 4);
- Duplicated of formers in CR position cabinets and signals transmission lines from each PR position cabinet to respective channel forming output signals in signals forming cabinet (see Figure 5);
- Duplicated of channel forming control signals in signals forming cabinets and control buses from each signals forming cabinet to all power control channels in power control cabinets (see Figure 6);
- Triplicate redundancy of connecting fields in manual input elements (keys, switchers, buttons) monitoring and control panel and lines connecting these elements to each signals forming cabinet (see Figure 2);
- Duplicated of CR position indication devices, one of which is placed in MCR, the other – in ECR, and capability to display data on each CR positions on the panel computer monitor, embedded in MCP, and on workstation monitors;
- Triplicate redundancy of SHC E&PRP primary power sources, duplicated primary and secondary power sources of operating stand-alone component parts;
- Duplicated of supply voltage transformers embedded in operating stand-alone component parts.

Emergency protection commands received by each channel (signals forming cabinet) from the respective channel of the first and second SHC E&PRP sets are connected in pairs in accordance with "OR" logical condition and multiplied with the help of active elements in the base and reserve safety signal forming channels (see Figure 4). Then these signals are sent to all power control channels in power control cabinets via separate electrical lines. In the base and reserve block of each power control channel logical processing of signals received via three independent lines from the base and reserve safety signal forming channels in first, second and third signals forming cabinet (by "two of three" condition). The base or reserve block removes alternating and direct current power supply from electromagnets of the controlled CR drive in case of presence of two or three protection signals at the input. Thus, commands from outputs first, second and third channels of the first and second SHC E&PRP preserved to end blocks, directly controlling electromagnet CR drives, besides, in each channel two independent inter-redundant ways for emergency protection command passing are provided.

For *diversity principle* realization during emergency reactor protection command performance has two different executive devices. One of them is SHC RG&IC itself, which by ERP command removes power at the base and reserve block power control channels outputs. Functions of the second executive device performs equipment, which by the same command of the first and / or second SHC E&PRP sets performs mechanical circuit disconnection, disconnecting of power supply all power control cabinets from alternating and direct current power supply.

Requirements to *personnel errors prevention* are regimented in SHC RG&IC documents in compliance with formulations of applied to it norms and regulations NP, 2000. They are related to identification and location of manual input and data visual display means location, diagnostic information imagery, protection from unauthorized access, compatibility and labeling plug-in component parts, operational documentation. Technical decision and organizational means were realized, which exclude the possibility of:

- Simultaneous removal of two SFC signals forming cabinets;
- Changing of CR misalignment set-point without personnel's warning;
- Selection of more than one CR group and more than six CR for manual control;
- Upwards group movement when operator performs pure condensate insert feeding;
- Unauthorized access to cabinets, their component parts, databases, software and archives.

Requirements, aimed at exclusion or mitigation of personnel's errors consequence are considered during development of embedded diagnostic and diagnostic information imagery means, as well as operator actions supporting means (human-machine interface).

Quality of functions performance is provided by rate setting and requirements fulfillment to accuracy and time characteristics, as well as to human-machine interface.

SHC RG&IC-R *accuracy characteristics* are set for sending to IRMS data on CR position, define of CR misalignment in each group and measuring of CR falling duration. Misalignment is calculated and displayed on the monitoring and control panel in digital and quasi-analog form of absolute units with 1% discretion. Absolute measurement error allowable limits of CR falling duration in operation condition are ± 0.01 s. Position indication error does not exceed 20 mm while using of stepwise sensors of control rod position (in case of other type sensors usage the error raises only on the intermediate sections border of rod working stroke, and is defined by sensor).

Requirements to *time characteristics* are regimented with regard to Ukrainian regulatory documents (see Chapter 3), compliance with SHC RG&IC-R set requirements confirmed during validation of deliverable complete set.

During *human-machine interface* development NP, 2000 requirements, applicable to SHC RG&IC-R, were realized: to information display devices (video monitors); to means of displayed and indication of data unreliability; to organization of visual system and video frame call; to signalization of arisen malfunctions, failures and errors; to acknowledgment of receiving and prohibiting of alarm messages sending; to conventional symbols used during data input, display and registration.

Stability of function performance is provided by SHC RG&IC-R operating stand-alone component parts resistance to environmental influence and mechanical (seismic) influence, as well as by immunity to change of primary power supply and to electromagnetic interference.

Environmental influence resistance requirements comply with set in Ukrainian norms and regulations for specified groups of operation conditions (E.2.2 and E.2.3 – see Chapter 3). SHC RG&IC-R compliance with the set requirements is confirmed during validation of deliverable complete set.

Generalized parameters of seismic influence (requested response spectrum), is according to maximum calculation earthquake (7 point) intensity (with regard to, which seismic category I device stability must be provided) and project earthquake with 6 point intensity (with regard to, which seismic category II device stability must be provided) are set in compliance with requirements GOST, 1998 (see Chapter 3), and are more severe in comparison with NP, 2000 requirements. Stability to seismic influence is proven by device prototypes test results.

During deliverable complete set validation were confirmed operating stand-alone component parts immunity to: electrostatic discharge; electrical fast transient / burst; surge; radiated radio frequency electromagnetic field; conducted disturbances induced by radio-frequency fields; power voltage fluctuation, dips, short interruptions and variations; power frequency variation; pulse and damped oscillatory magnetic fields; oscillatory waves; conducted common mode disturbances; alternating and microsecond impulse disturbances in ground circuits. Test disturbances parameters were defined for each type of disturbances in compliance with NP, 2000 and recommended International standards in a way by the test results to confirm the possibility of SHC RG&IC-R performance in premises with electromagnetic environment of medium severity.

Independence of performed functions is defined by preservation of capacity to perform the set functions in case of failure or removal of any redundant channel or any system connected with it.

For following of independence principle in SHC RG&IC-R is provided galvanic isolation of input-output circuits and power supply circuits with usage of optical separation devices; physical division of elements, which belong to different redundant channels, including placement of channel forming safety, output and control signals in separate cabinets; reserved channels power supply from different sources. In case of any SHC RG&IC-R component parts failure performance of adjacent systems (E&PRP system, RPwCUL&APP system, CIS and IRMS) is preserved, excluding functions for performance of, which the required data cannot be received due to SHC RG&IC-R failures. Any CIS and IRMS failures and single failures in SHC E&PRP and RPwCUL&APP systems do not influence the SHC RG&IC-R capacity to perform its functions. Means concerning following of independence principle, which correspond to the actual Ukrainian nuclear and radiation safety norms and regulations (NP, 2000) and international standards (IAEA, 2002 and IEC, 2011) are provided and realized.

SHC RG&IC-R meets requirements of Ukrainian fire regulations of designing nuclear power plants. The probability of fire in each operating stand-alone component parts not more than 10^{-6} in a year. Fire prevention means, assumed during developments, correspond to that regimented in NP, 2000 and NP, 2008,a Ukrainian norms and regulations.

Electromagnetic disturbance emission, radiated by SHC RG&IC-R operating stand-alone component parts during their switch-on, performance and switch-off, does not exceed the values, set in GOST, 1991 for information engineering equipment.

Approbation and implementation. Main technical solutions, elements base, hardware and software, which were intended to be used in SHC RG&IC-R, as well as methods of validation and testing at NPP were approved before the start of its development – in software-hardware complexes, developed and manufactured by RPC "Radiy" on base of common platform (see Chapter 1), which are successfully operated at Ukrainian NPP power units. The compliance with applicable safety requirements is confirmed by validation of deliverable complete set of SHC RG&IC-R.

SOLUTIONS AND RECOMMENDATIONS

Central part of rod group and individual control systems of WWER-1000 units was implemented by apparatus designed and manufactured by ŠKODA JS a.s. (Czech Republic) on the first stage of modernization at Ukrainian NPPs. Now these systems do not correspond to requirements in new Ukrainian and international regulations and standards and operator- "Energoatom" Company recommended to replace them on software- hardware complexes designed by Ukrainian organizations.

Software- hardware complexes for group and individual control (RG&IC-R) designed and manufactured by Research and Production Corporation Radiy, can be recommend for this replacement. This complex can be used not only from modernization of operating units, but for new units Khmelnitsky NPP 3 and 4 with increasing number of control rods.

FUTURE RESEARCH DIRECTIONS

The diversity principle supposes execution of emergency reactor protection command by two different ways. One of them is execution by SHC RG&IC, which described below. The second way is mechanical circuit disconnection, deenergizing all power control cabinets from alternating (base) and direct (reserve) current power supply, by the emergency reactor protection command.

In consequence of that, one of the directions of future activity for rod group and individual control systems modernization is elaboration and using operating stand-alone item (software-hardware complex), what assess CR drives power by direct and alternating power, diagnostic of power parameters and reliable mechanical disconnection of main and reserve supply circuit by command of emergency protection system and demonstrate its compliance with safety requirements on all stages of life cycle. Note, that "Radiy" Corporation is currently elaborating the same complex, what can be delivered together with or separately from SHC RG&IC.

CONCLUSION

As an actuation system that performs functions of emergency and preventive reactor protection, reactor power control and unloading, and commands send by the power unit operating personnel, the rod group and individual control system and its central part, the software-hardware complex SHC RG&IC-R, developed by the Research and Production Corporation Radiy, are considered. Besides the control functions, SHC RG&IC-R performs information functions required to support operating personnel and additional functions such as automatic diagnosis, notification of failures, archiving, displaying and recording of current and archive information.

The development and implementation of SHC RG&IC-R involves preservation of algorithms, priorities of control functions, control rod drive management principles, connections with other power unit I&C systems and peripheral equipment used in the operational rod group and individual control systems at Ukrainian NPPs. Modern information technologies, new electronic components and computer systems for data processing, storage, display and recording have improved consumer properties and operational reliability of the system upgraded on the basis of SHC RG&IC-R. All main and a number of auxiliary functions are based on field programmable gate arrays (FPGA), the electronic designs of which were developed and implemented by RPC "Radiy." The use of FPGA ensured high flexibility comparable with the capabilities of programmable computer aids and, at the same time, adequate predictability of the behavior and testability typical of hard-wired technologies.

Compliance with requirements of applicable nuclear and radiation safety regulations and standards is confirmed by the Ukrainian Nuclear Safety Regulatory Authority based on state review of the documentation and validation of deliverable complete set SHC RG&IC-R.

The modernization of the rod group and individual control system by replacement of obsolete and physically aging equipment of the central part of these systems with new software-hardware complexes is a promising area in ensuring the reliability, safety, and effectiveness of Ukrainian NPPs.

The software-hardware complex SHC RG&IC-R can also be recommended as a technical base for modernization of the rod group and individual control systems at WWER-1000 NPPs operated in other countries (see Chapter 8) and at new power units, including designs with an increased number of control rods.

REFERENCES

Gorochov, A. et al. (2004). *Explanation of neutron-physical and radiation parts in WWER design*. Moscow: Akademkniga.

GOST. (1991). GOST 29216. *Electromagnetic compatibility of technical means: Man-made noise from information technology equipment: Limits and test methods.*

GOST. (1998). GOST 30546.1. *Common requirements for seismic resistance of equipment, devices and other technical items and methods of their calculations*.

IAEA. (1999). INSAG-12. *Basic safety principles for nuclear power plants (75-INSAG-3, Rev. 1)*. Vienna, Austria: IAEA.

IAEA. (2000). NS-R-1. *Safety of nuclear power plants: Design: Safety requirements*. Vienna, Austria: IAEA.

IAEA. (2002). NS-G-1.3. *Instrumentation and control systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IEC. (2011). IEC 61513. *Nuclear power plants - Instrumentation and control important to safety - General requirements for systems*.

Nikituk, V. et al. (2004). *WWER control rod drives for nuclear power plants*. Moscow: Akademkniga.

NP. (2000). NP 306.5.02/3.035. *Requirements for nuclear and radiation safety information and control systems important to safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2008a). NP 306.2.141. *General provisions on the safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2008b). NP 306.2.145. *Nuclear safety regulations the reactors nuclear power plants with pressurized water reactors*. Kiev, Ukraine: State Nuclear Regulatory Committee.

ADDITIONAL READING

Bakhmach, E., Siora, A., Bezsalyi, V., & Yastrebenetsky, M. *Digital systems for reactor control: design, experience of operation.* Proceedings of the 16th International Conference on Nuclear Engineering ICONE16, 2008, Orlando, Florida, USA.

IAEA. (2011). NP-T-3.12. *Core knowledge on instrumentation and control systems in nuclear power plants. IAEA nuclear energy series, No. NP-T-3.12*. Vienna, Austria: IAEA.

Dunn, W. R. (2002). *Practical Design of Safety-Critical Computer Systems*, Reliability Press, Solvang. USA.

IAEA NP-T-1. 4 (2008). *Implementing digital instrumentation and control systems in the modernization of nuclear power plants*, IAEA, Vienna.

IAEA NP-T-1. 5 (2009). *Protecting Against Common Cause Failures in Digital I&C Systems*, IAEA, Vienna.

IEC 60980:1996. *Recommended Practice for Seismic Qualification of Electrical Equipment for Nuclear Power Generating Stations.*

IEC 61000-4-10:2001. *Electromagnetic compatibility (EMC) – Part 4-10: Testing and measurement techniques - Damped oscillatory magnetic field immunity.*

IEC 61000-4-11:2004. *Electromagnetic compatibility (EMC) – Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests.*

IEC 61000-4-12:2001. *Electromagnetic compatibility (EMC) – Part 4-12: Testing and measurement techniques - Oscillatory waves immunity test.*

IEC 61000-4-14:2002. *Electromagnetic compatibility (EMC) – Part 4-14: Testing and measurement techniques - Voltage fluctuation immunity test.*

IEC 61000-4-16:2002. *Electromagnetic compatibility (EMC) – Part 4-16: Testing and measurement techniques - Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz.*

IEC 61000-4-2:2001. *Electromagnetic compatibility (EMC) - Part 4-2: (Testing and measurement techniques - Electrostatic discharge immunity test.*
IEC 61000-4-3:2001. *Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity.*

IEC 61000-4-28:2002. *Electromagnetic compatibility (EMC) – Part 4-28: Testing and measurement techniques - Variation of power frequency, immunity test.*

IEC 61000-4-4:2001. *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques - Electrical fast transient / burst immunity test. Basic EMS Publication.*

IEC 61000-4-8:2001. *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test.*

IEC 61000-4-9:2001. *Electromagnetic compatibility (EMC) – Part 4-9: Testing and measurement techniques - Pulse magnetic field immunity test.*

IEEE Std 379 (2000). *Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*.

IEEE Std 344 (2004). *Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*.

KEY TERMS AND DEFINITIONS

Common Cause Failures: A simultaneous failure of two or more elements in different redundant parts due to one and the same cause, which can result in a failure of I&C function class.

Diversity: A property related to a group of two or larger number of I&C systems and SHC, which simultaneously and independently perform functions identical for achieved safety purposes and differ from each other by the operating principle, structure, applied component parts, software and / or other attributes or achieve the target goal in different ways.

Human-Machine Interface: The interface between operating staff and I&C system and computer systems linked with the plant. The interface includes displays, controls, and the operator support system interface.

Modernization: A set of actions for improvement of safety, functional abilities, reliability and / or technical and economic measures of an active I&C system related to substitution of individual components by more up-to-date ones and requiring changes in the accepted design and design and / or operational documentation.

Platform (Equipment Family): A set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). An equipment family usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software.

Safety Classification: Differentiation of the system or its components into classes, depending on their influence on NPP safety.

Single Failure Principle: A criterion which requires performing all specified functions in any postulated initiating event, combined with a failure of one (any) element independent from this event.

Chapter 11
Safety Parameters Display Systems

Vladislav Goldrin
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

ABSTRACT

The chapter contains a description of Safety Parameters Display Systems (SPDS) implemented at NPP units WWER-1000 of Ukraine. These systems were designed by Westinghouse Electric Corporation (USA). LLC "Westron" (Ukraine) took development and implementation of these systems. These systems were provided at 11 NPP units in the framework of the International Nuclear Safety Program with the support of DOE (USA). The general purpose of SPDS is to provide support for operators, when abnormality of NPP unit operational conditions must be determined rapidly. The chapter considers the purpose and the functions of these systems, specific features of the displaying information about the state of the functions, which are critical for NPP unit safety, and the structure of systems. Implementation of SPDS project at 11 units of Ukrainian NPPs is a good example of USA and Ukraine collaboration in the nuclear area. Organization of this large-scale modernization is described.

INTRODUCTION

The SPDS was created as part of the overall unit I&C system, which executes a large number of functions that are independent with respect to other individual I&C systems and is integrated with the existing systems at the design level of linkage.

SPDS realized critical safety functions on monitoring in all NPP operation modes with the aim of identifying the signs of violation of critical safety functions and definition of personnel actions which are priority from safety point of view.

SPDS displays minimized and group (from safety point of view) set of technological parameters which could quickly estimate state of NPP unit.

BACKGROUND

The development of the safety parameter display system (SPDS) was started at the time of the accident at the Three-Mile Island (TMI) nuclear power plant in 1979, which demonstrated the inadequacy of displaying information by traditional methods.

Following the accident at TMI, the regulatory body of the United States, the NRC, issued report NUREG-0696 (US NRC, 1981), which calls for the

DOI: 10.4018/978-1-4666-5133-3.ch011

use of an action plan for TMI to improve safety of nuclear power plants. This report sets the foundation for the safety parameter display system and the concept of critical safety functions. The basic function of SPDS is to assist the operator in quickly determining abnormal operating conditions.

Joint international safety analyses of Soviet-produced reactors revealed the existence of safety deficits in the man-machine interface for the WWER units.

PURPOSE AND FUNCTIONS

The goal of SPDS introduction was improvement of safety, reliability and efficiency of operation of nuclear power plant units by offering information support to main control room personnel and other technical personnel of NPP in evaluating the safety state in the unit by virtue of continuous monitoring of important parameters of the unit or calculating variables, which represent the safety condition of the unit. The main purpose of the SPDS is to offer assistance to the operator in quickly determining deviations in unit operation.

In this case the SPDS can be used to analyze and diagnose causes of the onset of disturbances in operation of the generating unit, and to identify corrective actions.

The SPDS offers information support to the operator during normal operation of the nuclear power plant and during emergencies:

1. To evaluate the ongoing condition of nuclear power plant safety;
2. To evaluate safety margins and conditions of operation before triggering reactor protection system;
3. To evaluate the state of limits and safety conditions of operation after initiation of protection and other safety systems;
4. To evaluate effectiveness of the operation of protection and other safety systems;
5. To evaluate the need for corrective actions, which are aimed at prevention and alleviating design and accidents.

The advantages of presenting information in the SPDS are the following: information distributed to the modular control panel is presented in concentrated form and in a single system; the operator can use associative thinking, and not complex computing operations and analysis to make decisions in stressful situations; the SPDS directly presents to the operator values of safety margins for changing parameters up to the emergency protection initiating settings; it concentrates a large amount of information, using special techniques of image displays, thereby making the information perception process simpler and quicker.

Because of significant differences of the limits for normal and safe operating conditions before and after shutdown of a reactor, the SPDS employs three upper level polarographic video frames.

The polarographic video frame “narrow range” is intended to monitor deviations in the production process from normal operation and to evaluate safety and integrity of protective barriers from radioactive releases of the reactor unit in full power operating modes. The video frame offers assistance to the operator in eliminating the reason of a normal operation deviation.

The polarographic video frame “wide range” is used to monitor safety and integrity of protective barriers from radioactive releases in all modes after shutdown of the reactor unit. The video frame helps the operator in preventing worsening of normal operational deviation.

The polarographic video frame “cold shutdown” is used to monitor safety of the reactor unit and integrity of protective barriers from radioactive releases in cold shutdown mode, including fuel reloading mode.

An example of polarographic video frame of the SPDS (narrow range) is shown in Figure 1. State of limiting systems, radioactivity, neutron power, loops in operation, etc. are displayed on the video frame.

Insofar as a human easily recognizes differences in distortions in symmetrical geometric figures, a true (in normal state of the production process) polygon is used as the basic graphic signal for displaying deviations of the production process.

The lengths of segments (characteristic vectors), which connect the center of the polygon to its corners, will represent values of the generalized safety parameters, that is those parameters from the full set existing in the SPDS, which more generally characterize the safety condition.

Each electronic line on the video frame depicts a certain scale of generalized safety parameters. Standardized values of critical operating parameters are shown on the scale in vector form.

The value indicating scales of each parameter are standardized in such a way that the visible length of all characteristic vectors is identical in the range of values of the corresponding parameters that are accessible in a given mode of the generating unit. The minimal value of the corresponding parameter is 0.6 of the full length of any characteristic vector. Positive deviations from the norm drive the ends of the vector away from the center of the figure. Negative deviations, on the contrary, bring them closer to the center of the figure. Thus, for all parameters the lower limit is depicted closer to the center of the figure.

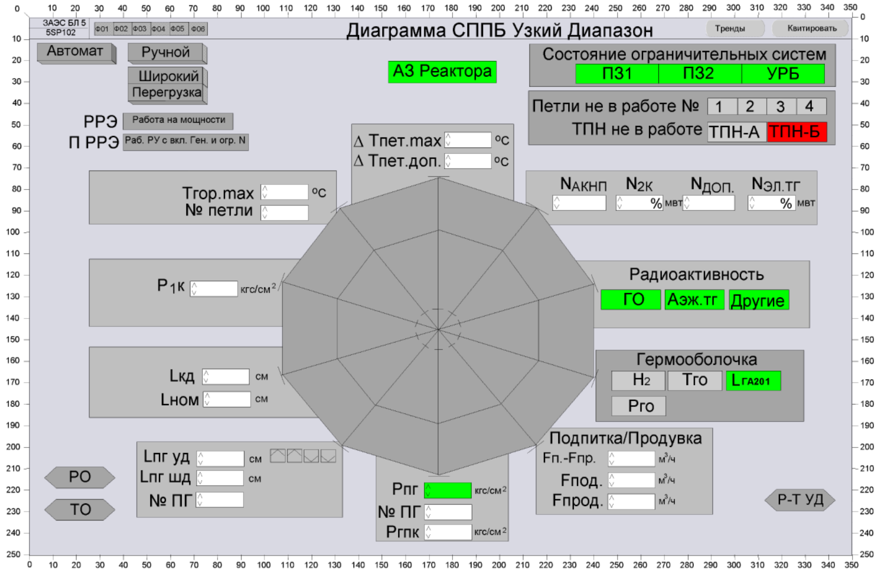
Segments that connect the ends of the characteristic vectors in normal state form a true geometric polygon on the screen.

For each characteristic vector of polar diagrams, the upper and lower limits are shown, which represent: regulated limits (operating limits) for the "narrow range" and "cold shutdown" diagrams; emergency limits (design limits of safe operation) for the "wide range" diagram.

The instantaneous value of a critical parameter is represented by the end point of the characteristic vector and the line that connects the end points of the vectors forms a polygon. When the parameters differ from the norm, a different geometric shape appears on the screen.

Evaluation of a critical situation is simplified and maximally minimized, that is the operator's task reduced to comparing two geometric shapes -- a polygon of instantaneous values of generalized safety parameters and a symmetrical polygon of nominal values of parameters.

Figure 1. Polarographic video frame "narrow range" (picture from the screen)



The visual comparison of shape allows one to quickly establish conformity of the instantaneous condition of an object to the expected condition and to determine the presence of a deviation from the norm. In this case the identification of "abnormal location" or, in other words, determination of the fact that there has occurred a deviation from normal, it is accomplished along the vector which caused distortion of the shape of the polygon of instantaneous values of parameters.

The polarographic representation of critical parameters of safety offers the possibility of acquiring additional practical experience in evaluating the instantaneous state of an object or likelihood of damage to protective barriers, because the making of decisions and evaluation of situations by the operator will be improved due to the recognizable nature of the polar diagrams and lighting up of only difference of parameters.

In order to evaluate safety in accordance with requirements of USNRC, 1981 five critical safety functions have been distinguished:

1. Reactivity control;
2. Reactor core cooling and heat removal from primary system;
3. Reactor coolant system integrity;
4. Radioactivity control;
5. Containment integrity.

SPDS DESCRIPTION

Hardware Components

The central part of SPDS is the software-hardware complex (SHC), which was configured by LLC "Westron" based on equipment of Westinghouse Electric Corporation (United States) (Kolesov, 2000).

The SHC accomplishes the collection of data that form the basis for calculation of different physical quantities, monitoring, signaling, recording and subsequent display of all assigned input/output signals and calculated parameters on video frames and in the form of trends.

Westinghouse Electric Corporation in 1982 produced a family of equipment WDPF (Westinghouse Distributed Process Family), which is based on fully distributed architecture and data main bus with deterministic protocol. In 1990 Westinghouse developed the WDPF-II family with improved main data bus Westnet II and expanded set of peripheral equipment, supplied by leading world companies.

WDPF-II is a structured set of devices, which is oriented to use as the equipment base in configuration of SHC for information and control systems in different sectors of industry.

LLC "Westron" conducted acceptance inspection of the received equipment, configuration of the SHC for specific customers, testing, acceptance, production of technical documentation, and startup and troubleshooting work. This allowed them to assure adaptation of the SPDS to requirements of regulatory documents in effect in Ukraine (in number of cases, requirements differ from requirements of national standards of the United States, to which the WDPF-II developers were oriented).

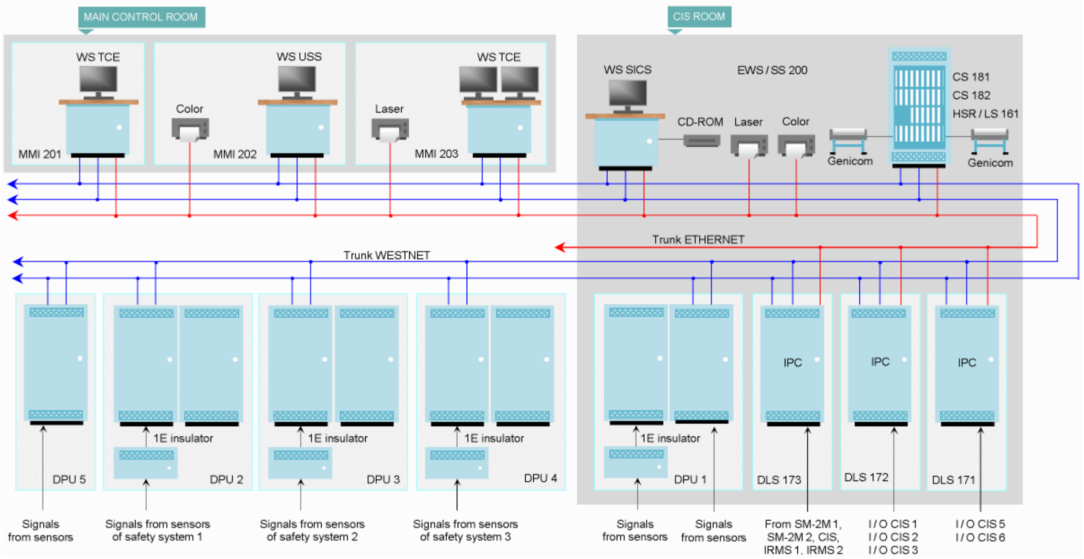
The concept of SHC creation called for transformation of serial (hardware and software devices of WDPF-II) and commercial articles of leading world electronic manufacturing companies to unit articles (SHC with software, service equipment and operating documentation).

STRUCTURE

The principles of constructing the SPDS for nuclear power plant units of Ukraine are set forth in the example of the SPDS of Zaporozhe NPP unit 5 (Figure 2).

As input information, the SPDS uses signals of existing standard sensors, new sensors, which are installed according to the SPDS design, and existing I&C systems in the generating unit (computer information system – CIS, in-core reactor

Figure 2. The structural scheme of the Zaporozhe NPP SPDS



monitoring system – IRMS, neutron flux monitoring system – NFMS, radiation safety control system – RSCS, reactor control rod system – RCRS).

The signals of systems external to the SPDS are transmitted over digital communication channels. The SPDS is made in the form of an integrated, distributed open system on the basis of local area networks (LAN) of two kinds: data LAN and information LAN.

The data LAN is used to transmit the required amount of production information between subscribers of the LAN at a predetermined access time for each subscriber. The LAN made by Westinghouse Corporation, the type Westnet II+, is used as the data LAS.

The information LAN is used to transmit large files of production and service information between subscribers of the network and, if necessary, to external users. A standard LAN of the Ethernet type is used as the information LAN.

The LAN combine independent microprocessor sub-complexes, which use intelligent hardware input/output devices, terminal units and, if necessary, signal normalizers.

Structurally the SHC of the SPDS is a two-level system.

The lower level stations perform input of continuous and discrete signals from sensors, reception of data from other unit systems and primary processing of the derived information. The upper level stations perform more complex calculations, ensure maintenance of the man-machine interface, perform the storage, display, recording and archiving of data.

The upper level is comprised of workstations (WEStation) that are specialized in accordance with functions fulfilled, which are hooked up to both the Westnet II+ and Ethernet main buses.

Upper level stations are stations on the base of workstations made by Sun Microsystems Company with real-time operating system Solaris™ of the UNIX family

Base workstation crates and industrial personal computers (IPC) are placed in the cabinets, which perform computing operations that require high speed, considerable volume of on-line memory and access to databases in real time (thermotechnical, economic and other calculations, inspection of protection devices and interlocks and so forth).

The IPC composition includes: built-in systems module with processor, PCI/Ethernet local main bus adapter, installed in the systems unit; built-in video monitor; built-in symbolic keyboard.

The upper level equipment includes: operator station MMI 201, which is included in the workstation (WS) of the turbine control engineer (TCE); operator station MMI 202, which is part of the unit shift supervisor (USS) workstation; operator station MMI 203, which is part of the reactor control engineer (RCE) workstation; engineer station (server EWS/SS 200), which is part of the shift of I&C supervisor (SICS) workstation in the CIS room; archiving station/documentation server HSR/LS 161, which are included as part of the shift I&C supervisor workstation; computer servers CS 181, CS182, which are part of the shift I&C supervisor workstation.

Equipment of the upper level also includes single-color laser printers Laser Ptr that can be hooked up directly to the main bus and are installed in the CIS room and main control room. They are used to print reports in the form of text and graphs and color HP 1200C (Color Ptr) ink-jet printers for outputting screen copies to the printer, and also Genicom printers, which are hooked up to the HSR/LS 161 server.

Low level stations – sub-complexes for gathering and processing data – are implemented on the base of DPU (distributed processing unit) collection devices serially produced by Westinghouse Corporation. The DPU is a two-channel (redundant) microprocessor system, each channel of which contains: microprocessor; mathematical co-processor; specialized logic co-processor; sentry timer; electrically erasable programmable storage unit (flash memory); on-line memory device; Westnet II local network controller (with outputs for connection to both Westnet II main buses); RS-232 sequential port for connecting to the servicing portable computer; internal bus Multibus I; internal (local) memory expansion bus; one or two external input-output bus controllers; secondary power supply.

One, two or three individual DPU are located in a floor cabinet. Input/output modules are placed in the same DPU cabinet (up to 36 modules) and/or in expansion cabinets (up to 48 modules in each one) and are connected to DIOB buses. Direct current power of the modules comes from two secondary sources (main and backup), which are installed in the DPU cabinets and then the expansion cabinets.

In addition to the input/output modules of the analogue and digital signals "Westron" developed and manufactured special modules (programmable logic controllers) for inputting data into the DPU along digital channels from other I&C systems of the unit.

The DPU gathers information, converts input signals to unified digital format, primary analysis (inspection of output of parameters beyond limits of maximum values, analysis of emergencies, generation of warning and emergency messages) and issues dated to the Westnet II network. Technical diagnosis, automatic restart, possibility of configuration, inspection and change of DPU settings in autonomous mode and in the operating process (along the Westnet II man bus) are also provided.

The lower level equipment includes: stations for distributed collection and processing of signals from the DPU1-DPU4 sensors together with cabinets of the galvanic signal insulating devices (1E insulators); the stations DPU5 without a cabinet for such devices; the servers DLS 171, DLS 172, and DLS 173 for communications with the Westnet bus of associated systems along the digital channels.

Associated systems with such connections include: the "Kompleks-Titan" computer information system (connection with high level complexes SM-2M1, SM-2M2 and low level input/output complexes KSO1-KSO3, KSO5, KSO6); in-core reactor monitoring systems (communications with IRMS1 and IRMS2); the hydrogen monitoring system (HMS).

The DPU centers receive signals from sensors: safety systems – DPU2, DPU3, DPU4; normal operating systems of the reactor compartment – DPU1; normal operating systems of the turbine department – DPU5.

The 1E insulators developed by Westinghouse are used to connect the DPU2-DPU4 with signal sources of the safety systems, and also to connect the DPU1 to signal sources of safety class 2 in normal operating systems of the reactor compartment.

In order to organize digital communication channels with associated systems, industrial personal computers are used that are built in cabinets of the communication servers.

Approximately 700 parameters arrive directly from the sensors and about 1400 through the digital data transmission channels from the existing computer information system.

Redundancy (duplication) of individual most important blocks and combining the execution of functions of certain functional components (servers) in devices of the same station is provided.

The structure of the system and hardware devices used offer the possibility of its expansion in the future by means of: increasing productivity and expanding the functional capabilities with the introduction of additional personal workstations and functional service of the SPDS in connection with autonomy of each of the station, which is assured by the modular structure of the system and use of the "client-server" concept; increasing the productivity of individual stations of the network by replacement of processors with more productive ones, building up the on-line memory, connection of additional magnetic and optical disks and peripheral devices; connection to the Westnet bus of additional sources of incoming data by using communication devices with the object from the WDPF set of equipment; use of widely disseminated commercial software products (Sun OS/C/Ethernet open windows); combining several Westnet networks in a single system.

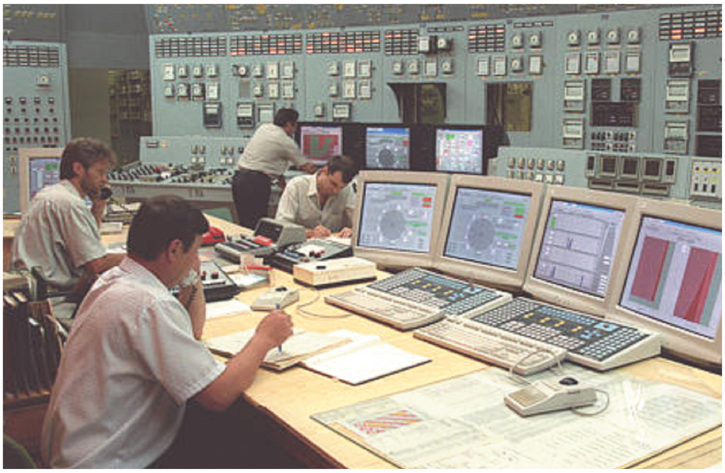
A general view of the SPDS at the main control room is given in Figure 3.

Software

Software can be classified in the following manner based on its level of approval: standard software WDPF-II developed previously by Westinghouse, approved for different projects, including nuclear power plants; previously developed commercial systems software of other foreign developers; software created for the first time especially for SPDS.

One particular feature of SPDS is the presence of a software server (EWS/SS200), which stores a standard reference set of all programs. Loading

Figure 3. General view of the SPDS at the main control room



the programs into DPU memory and workstations is accomplished from the EWS/SS200 over the Westnet II local network. Software for engineering stations (EWS/SS200 and EWS/CIU207) supports functioning of the SPDS.

The systems software includes: operating memory iRMX; operating system MS-DOS; operating system Solaris; protocol support drivers; peripheral device drivers; drivers of interface modules; Russification programs.

The display of information in video frames is implemented according to the technological hierarchical principle "from the general to the particular."

The technological process video frames are separated into five levels of hierarchy. Know-how in the display of general information comes primarily from upper level video frames, on which information is displayed in the form of polar diagrams – polygons.

The video frame hierarchy includes:

- **Upper (First) Level Video Frames:** Unit safety;
- **Second Level Video Frames:** General state of the unit;
- **Third Level Video Frames:** Effectiveness of unit functions;
- **Fourth Level Video Frames:** State of the unit systems;
- **Fifth Level Video Frames:** Sensor readings.

The most general information on safety parameters of the generating unit is on upper level video frames. The lower level video frames give tehnological process information in detail.

The set of computer subsystem programs produces computations for execution of the following main functions:

- Calculation of parameters displayed on the polygon-diagrams;
- Determination of the condition of critical safety functions;
- Calculation of generalized safety parameters;
- Calculation of reactor power output achieved;
- Determination of the number of working turbine feedwater pumps;
- Power output balance;
- Core condition monitoring;
- Special calculations for the NPP unit;
- Reliable determination of heat carrier temperatures;
- Determination of the number of working loops;
- Radioactivity monitoring;
- Calculation of first loop leakage;
- Mass balance;
- Monitoring the level in the pit;
- Recording actuation of the protection system;
- Determination of constants for the NPP unit;
- Determination of the condition of equipment;
- Monitoring the condition of the NPP unit warm-up and cooling down;
- Reliable determination of NPP unit parameters;
- Processing of neutron parameters;
- Monitoring parameters of state of the containment;
- Calculation of thermodynamic parameters of water and steam.

The calculations are also performed for the following auxiliary functions:

- Analysis of redundant measurements;
- Correction of flow rate and level parameters;
- Determination of the rate of change of parameters;
- Averaging of parameters over time.

ASSURANCE OF COMPLIANCE WITH SAFETY REQUIREMENTS

The SPDS is defined as a normal operating system that is important for safety, and is given the classification designation 3N, according to Ukrainian Regulation (NP, 2000,a).

Regulatory requirements of Ukraine (NP, 2000, b) for information and control systems that are important to safety of nuclear power plants were introduced in 2000. However, even before their introduction, the SPDS developers were familiar with the requirements contained in the draft of this document and took them into account in creating the systems.

United States requirements for such systems as the SPDS are described in NUREG-0696 (USNRC, 1981). Subsequently the IEC standard 60960 (IEC, 1988) was issued, which extends directly to safety parameter display systems and was harmonized with the criteria for SPDS in NUREG-0696.

In evaluating the safety of SPDS a comparison of requirements of the aforementioned documents was carried out. Priority was given to regulatory requirements of Ukraine.

The following sets of requirements were taken into consideration:

- For reliability of functions execution;
- For quality of functions execution;
- For stability of functions execution, etc.

Reliability Assurance

The reliability of SPDS assures fulfillment of the requirements:

- For reliability measures;
- For adherence to the redundancy principle;
- For protection from common cause failures;
- For technical diagnostics.

SPDS measures of reliability is brought about by: high reliability of the main hardware and software components of the SHC, which are supplied by leading foreign companies and have proved themselves reliable over many years of use, including use in NPPs; duplication of microprocessor components in all lower level stations (DPU); duplication of the most critical stations of the upper level (for example, the presence of archiving/documentation servers HSR/LS 165 and HSR/LS 166).

Analysis of operating reliability has confirmed that SPDS reliability measures are at the level of or above design estimates.

Redundancy is one of the main architectural features of SPDS, which assure preservation of its operation when there is failure of any of the main components.

The Westnet II local network has two parallel operating main buses, along which the same data are simultaneously transferred. The failure of one of them does not disturb the possibility of data exchange, which is accomplished over the other (good) main bus. If there is failure of the main computing server an identifier of the failure is generated, the main server automatically converts to autonomous mode, and the redundant server – to main mode. In a similar way one can ensure stations of the DPU when there is a failure of one of the two redundant channels.

Data display devices in the operator stations of the main control room are not backed up formally, but if there is a failure of any of them the possibility of observation is retained due to their redundancy at each workstation.

Common cause failures are eliminated by the adopted measures of redundancy, resistance of hardware devices to possible disturbances of operating conditions and action of anomalous natural phenomena.

The disappearance of voltage in the supply feed line was examined as one of the probable common factors. The DPU resistance to such interruptions of electric power is assured by the fact that each channel (main and backup) is powered from its own secondary source, while these sources are hooked up to two different primary electric power supply networks. Power for the input/output modules of analogue and digital signals is also made redundant in this manner. In this case the failure of any network does not lead to disturbance of DPU functioning, because power of one of the channels is preserved. For the same reason, redundant equipment of the higher level, which are supplied directly from the 220 V alternating current network, are hooked up to different networks of the primary electric power supply. Power of non-redundant operator stations is arranged so that if there is failure of any one of the networks and each workstation serviceability is retained by any one of two operator stations (hooked up to the good network).

Hardware diagnostic devices of SHC and the design solutions adopted ensure the possibility of quickly discovering failures and timely restoration of serviceability of any stations. In particular, the replacement of failed modules in the DPU can be done without disconnecting power and does not require installation following replacement.

DPU technical diagnosis is achieved by hardware devices (watch dog) and diagnostic programs as part of the library of standard programs, which are supplied by Westinghouse (level of diagnostics is up to one interchangeable module). Technical diagnostics of higher level stations is achieved by programming devices of the workstations and commercial personal computers. Diagnostic messages are transmitted over the local network and are displayed on the workstation video monitors.

Quality of Functions

Requirements for quality of functions include:

- Accuracy requirements;
- Requirements on temporal characteristics;
- Requirements for the man-machine interface.

Accuracy of the nformation functions is defined by the accuracy of sensors with continuous (analogue) output signals and measurement channels of the SPDS, which accomplish conversion, storage, transmission and display of data in digital form. In this case the main part of the error of information system measurement channels is that due to errors of sensors.

Limits of acceptable value of the assumed error rate of the SHC measurement channel under operating work conditions do not exceed ± 0.5% for signals of the thermocouples and thermistors ± 0.3% for signals of sensors with uniform current and voltage output.

For the inputting and conversion to digital code of signals from sensors in the measurement channels of the SPDS highly accurate modules QRT are used (for the input of four signals from the thermal resistance converters) and QAX (for input of 12 channels from the remaining sensors). Automatic calibration with "zero" correction and conversion factor of all conversion channels of input signals of a given module is accomplished every 8 seconds in the QAX modules and every 9 seconds in the QRT modules, that is built into the microcomputer modules. Limits of acceptable values of the induced error rate of signal conversion in the QAX or QRT module do not exceed ± 0.1%, and the "zero" drift per month is not more than ± 0.002%, long term drift is not more than ± 0.02%.

Temporal characteristics of the SPDS:

- Duration of the data input cycle from sensors of continuous and discrete signals (with deterministic access) – 0.1 and 1.0 seconds;
- Time resolution capability for input of continuous and discrete signals -- not more than 0.02 seconds;
- Rate of data refreshing, displayed on monitor screens, once per second;

- Rate of data transfer over the local Westnet II network -- 16,000 parameters per second, etc.

In order to display information at workstations of operating personnel, color video monitors are used with diagonal screen of 20 inches and 27 inches, resolution capacity of 1152 x 900 dots, number of colors 256. For the input, display and recording of data one uses conventional designations (including abbreviations and acronyms), which are convenient and understood by personnel and do not require additional deciphering.

Stability of Functions

Requirements for stability of functions include:

- Requirements for resistance to external influences;
- Requirements for electromagnetic compatibility (noise tolerance);
- Requirements for protection from unauthorized access, etc.

The stability of functions was evaluated on the basis of requirements of regulatory documents for nuclear safety, which were in effect in Ukraine at the time of SPDS introduction.

Resistance to external influences assures fulfillment of the stipulated functions (to the assigned extent and with regulated characteristics) under SPDS operating conditions and with disturbances of working conditions caused by: failures of supporting systems, which ensure operating working conditions; disturbances of operating mode of powerful electric engineering units; anomalous natural phenomena (e.g., earthquakes).

External influencing factors of the environment are characterized by working values and limiting values, which can occur in a limited amount of time, for example during failures of ventilation, air conditioning systems and so forth. Generalized working and limiting values of external influencing factors of the environment are determined according to (NP, 2000,b) depending on the operating condition group.

A comparison of these values with the requirements reveal that under the operating conditions in which upper and lower level stations are arranged, the external influences cannot influence their fitness for work and technical characteristics. However, compensatory measures were taken so that the limiting values of temperature and humidity in this space would not exceed acceptable limits for workstations.

The SPDS, as a system of safety class 3, is assigned to the category of seismic stability II and should fulfill the stipulated functions to the assigned extent with characteristics regulated in the specifications after action of vibration and mechanical shocks, which are caused by a design earthquake at the NPP site. For example, the intensity of a design earthquake for the site of the South-Ukrainian NPP is determined to be a grade of 6. Considerably more rigid requirements for seismic stability of the DPU have been established in the specification – grade of 8 for installation at level up to 10 meters. The conformity to these requirements is confirmed by test materials submitted by Westinghouse. For commercial items (workstations, video monitors, peripheral equipment and so forth), which are used as part of the upper level stations, additional reinforcement of items installed on work surfaces of table sand pedestals was stipulated as a compensatory measure.

Electromagnetic compatibility calls for stability of all component parts of the SPDS with respect to the action of interference from the power grid, special grounding loop, along the transmission circuits of signals, communication lines, local networks, and also in the space of the premises.

Stability requirements with respect to the following kinds of interference have been established in the specifications: discharges of static electricity to the frame, control members and external shields of cables; microsecond impulse interference in power circuits; nanosecond pulse interference to information circuits and power circuits; magnetic fields of industrial frequency, resistance to radiation radio frequency interference, dynamic changes of electric power supply voltage, pulse magnetic fields, brief sinusoidal microsecond pulse interference in protection and signal grounding circuits.

Protection from unauthorized access is assured in SPDS: by introducing identification codes, which determine authorities of users and list of devices and functions, which are accessible to each of them; archiving and recording of all personnel actions, which are connected with the chains of software and database; use of passwords (codes) for permission to the most critical actions; use of special locks on doors of supporting structures and their seals.

IMPLEMENTATION OF SPDS PROJECT

The SPDS project was implemented for all 11 WWER-1000 units of Ukrainian NPPs in compliance with the "Agreement between the Government of the United States and the Government of Ukraine Concerning Operational Safety Enhancement, Risk Reduction Measures and Nuclear Safety Regulation for Civilian Nuclear Facilities in Ukraine."

The complexity of implementation of the plan, which embraces SPDS at all WWER-1000 generating units, was determined by the following circumstances: large number of systems are being introduced; lack of SPDS at nuclear power plants of Ukraine with WWER-1000 reactors and, consequently, difficulties in determining the goals and tasks of the system; lack of regulatory documents that are in effect in Ukraine, which contain requirements for SPDS; differences in safety classification and in general regulatory requirements for safety in Ukraine and in the United States; need to develop the functional design used in SPDS.

Implementation of this project required the combined efforts of several organizations (Figure 4). Each of the participating organizations had performed the following tasks in the successful implementation of the whole program.

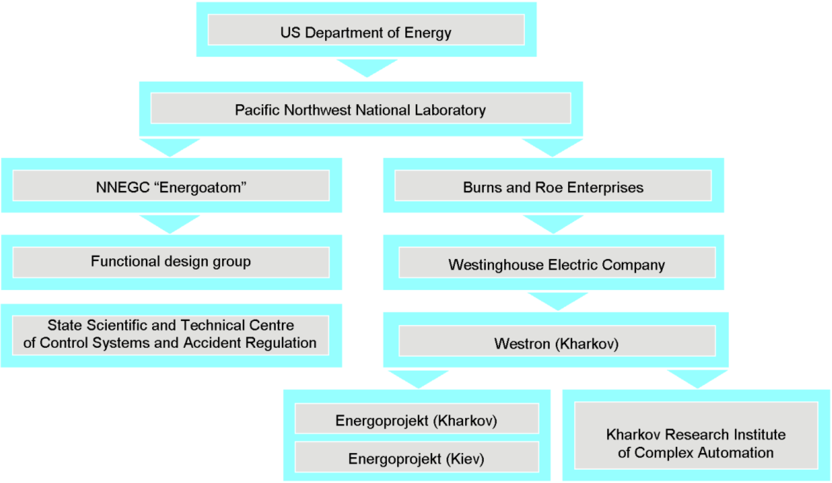
From the American party, the following organizations participated in the work:

- **US Department of Energy:** Sponsor of whole program;
- **Pacific Northwest National Laboratory:** Project management and general management for all contracts in Ukraine;
- **"Burns and Roe":** Technical management of project, signing of contracts with vendor SPDS;
- **"Westinghouse Electric Co."**: Vendor of computer equipment and components of hardware, basic application software, system software, instrumentation tools to Ukraine.

From Ukrainian party, the following organizations participated in the work:

- **National Nuclear Energy Generating Company (NNEGC) "Energoatom":** Organization management of installation and commissioning, development of input data on the functional part of the projects (work management of the group of functional design), organization of the training of NPP personnel;
- **Consortium (LLC) "Westron":** Designer of technical project SPDS, digital channel SPDS with unit I&C systems, integration and testing tasks SPDS equipment, programming of video frames, original application and configuring of basic software, training NPP personnel operation and service of hardware and software, backup service SPDS over a period of operation;
- **Kharkov and Kiev Institutes "Energoprojekt":** Development of con-

Figure 4. Interaction of organization, participated in SPDS elaboration


US Department of Energy
Pacific Northwest National Laboratory
NNEGC "Energoatom"
Burns and Roe Enterprises
Functional design group
Westinghouse Electric Company
State Scientific and Technical Centre of Control Systems and Accident Regulation
Westron (Kharkov)
Energoprojekt (Kharkov)
Energoprojekt (Kiev)
Kharkov Research Institute of Complex Automation

nection projects SPDS to design and construction documents;

- **Kharkov Research Institute of Complex Automation:** Development of software of CIS "Komplex Titan" for its support conntion with SPDS on digital channel;
- **State Scientific and Technical Centre of Control Systems and Accident Regulation:** Development control examples for validation algorithms of functional design.

State Scientific and Technical Centre for Nuclear and Radiation Safety (SSTC NRS) fulfilled expert reviews of SPDS nuclear and radiation safety.

A special Ukrainian–USA organizing committee was created to coordinate the implementation of the project at the first steps of SPDS elaboration.

One should pay particular attention to the work of the functional design group. This group was formed of representatives of nuclear power plants and specialists of different organizations. Westinghouse Electric Corporation conducted training for members of the group in modern information technologies, which were used in developing the SPDS. In turn, the members of this group brought to the project knowledge of the equipment, particular features of the production process of generating units of each of the nuclear power plants of Ukraine.

The first stage of the project was the introduction of the SPDS for two units – number 5 of the Zaporozhe NPP and number 1 of the Khmelnitsky NPP. The SPDS project in unit number 5 of Zaporozhe nuclear power plant is considered basic (prototype), because this unit has the greatest similarity with the majority of Ukrainian WWER-1000 units. The SPDS of unit number 5 of the Zaporozhe NPP included a sufficient volume of hardware and software devices for development, configuration and testing of the SPDS functions.

Differences of the SPDS projects for the different NPP units were determined: by certain differences in technological schemes and in the composition of the technological parameters; differences such as unit types and possibilities of organizing interfaces with the systems; certain distinctions in functional design (composition of video frames and their particular features, determined sometimes by technological differences, sometimes by the point of view and experience of personnel of each nuclear power plant.

The greatest differences from the basic design and SPDS of other NPP units is that of the SPDS of generating units number 1 and number 2 of South-Ukrainian nuclear power plant (WWER-1000 small series generating units). This pertains especially to SPDS of unit number 1, which was integrated into the computer information system, previously built on the basis of the same hardware devices, and similar in structure to the basic software used (Designers of this system were "Westinghouse" and "Westron").

In spite of the differences, the main requirements, functions and design principles of the SPDS were common for all generating units.

Specifics of the SPDS safety evaluation for nuclear power plants of Ukraine (Anikanov, 2003; Brenman, 2006) were determined by the following factors:

- Fundamental novelty of the system and its functional purpose that had no analogues in designs of Ukrainian nuclear power plant units;
- Development of basic hardware and components in accordance with regulatory documents of the United States;
- Need to compare requirements of regulatory documents effective in the United States and in Ukraine;
- Necessity of supplementing initial requirements for SPDS in the conforming specifications (document of Westinghouse Corporation) with special technical requirements, which supplement the conforming specifications to the full extent of the requirements, which are regulated by Ukrainian standards for the feasibility study for the system.

In evaluating the safety of SPDS, in accordance with the strategy for introducing the system at nuclear power plants of Ukraine, the following sequence of expert analyses was undertaken:

- Expert analysis of designs of the basic systems (for generating unit number 5 of Zaporozhe nuclear power plant, for unit number 1 of the Khmelnitsky nuclear power plant);
- Expert analysis of the designs of the remaining systems with consideration of the results of the expert analysis of the basic systems and differences of remaining systems from basic ones.

The greatest scope of documents was considered for basic systems:

- System conformal specification;
- Technical specifications for hardware complex based on which spds were developed;
- Reliability analysis report;
- Documentation on serial hardware supplied by Westinghouse;
- Design for SPDS link to operating equipment;
- Documents on tests on the supplier's site, including verification and validation documents;
- Preliminary safety analysis report;
- Documents on on-site tests;
- Pilot operation program and results;
- NPP Technical Solution with permission for putting into pilot operation;
- Final safety analysis report;
- NPP Technical Solution with permission for putting into stationary (permanent) operation.

More limited scope of documents on SPDS for other units was considered:

- Conformal specification with special supplementing technical requirements;
- NPP testing program and guideline;
- Safety analysis report;

- NPP Technical Solution with permission for putting into stationary (permanent) operation.

In compliance with regulatory safety requirements of Ukraine, the SPDS was classified as a safety-related normal operating system – classification notation 3N.

The SPDS developers were aware of regulatory requirements of Ukraine (NP, 2000,a; NP, 2000,b) considered their requirements in system development process.

Requirements for SPDS are set forth in US document (USNRC, 1981) and international standard (IEC, 1988), which applies to all safety parameter display systems; the safety criteria in this standard agree with the SPDS criteria from NUREG-0696.

In the SPDS safety assessment, Ukrainian regulatory requirements on safety and requirements of NUREG-0696 and IEC 60960 were compared. Priority was given to regulatory requirements of Ukraine.

The following groups of requirements were taken into account in the safety assessment of SPDS referred to safety systems of class 3N:

1. Reliability of functions performed;
2. Quality of functions performed;
3. Absence of impacts on other systems;
4. Stability of functions performed;
5. Procedures for confirmation of compliance with safety requirements.

The SPDS were implemented at Khmelnitsky NPP-1, Zaporozhe NPP-1, 2, 3, 4, 5, 6, Rovno NPP-3 and South-Ukrainian NPP-1, 2, 3.

It should be noted that in spite of some differences of the national regulatory framework of US as used in the development and implementation of SPDS from the Ukrainian regulatory framework, there had been no special difficulties in understanding between the developer (supplier) of the systems and operating organization on the one hand, and the Ukrainian regulatory authority and its technical support organization SSTC NRS on the other hand in the safety assessment for SPDS implementation at Ukrainian NPPs.

Solutions and Recommendations

Safety parameters display systems, which are described below, are separated from another individual I&C system - unit computer information systems (CIS). Both systems – SPDS and CIS – give information to personal for NPP unit control.

SPDS exerted positive influence on NPP safety; a lot of instruction for NPP personal were elaborated specially for using with SPDS.

The most parts of CIS “Complex-Titan” was elaborated in 1985-1990: there was USSR design with old hardware components. There was only one exception – CIS of South-Ukrainian NPP-1, which was the modification of old CIS. Modernized system was elaborated by “Westinghouse Electric Company” and LLC “Westron” (as SPDS) and used hardware and software similar as SPDS (Emphasize, that CIS and SPDS of South-Ukrainian NPP are independent systems), but SPDS and CIS of South-Ukrainian NPP-1 have some level of integration.

Experience of SPDS operation confirmed advantages of further integration CIS and SPDS. All new CIS in Ukraine was integrated with SPDS.

FUTURE RESEARCH DIRECTIONS

The set of critical safety functions began to form after the TMI accident. The Fukushima-1 lessons shown that it is necessary to introduce new safety functions in addition to the existing ones. One of these functions is spent fuel pool monitoring.

Correspondingly, a set of critical functions in SPDS have to be expanded. New functions have to be included to SPDS.

CONCLUSION

SPDS were implemented at all Ukrainian NPPs. Implementation of SPDS at Ukrainian NPPs has been realized jointly by the USA and Ukrainian companies according to intergovernmental agreement.

Purpose of SPDS as system for personnel information support and importance of SPDS for unit safety assurance are considered in this chapter. Peculiarities of presentation of information about technological process and state of unit safety functions (according to US NRC, 1981), structure of SPDS hardware and software are described.

SPDS project is a good example of cooperative activity of the US companies ("Westinghouse," "Burns and Roe," US DOE) and Ukrainian NPPs, design organizations, regulatory authority and technical support organization (State Scientific and Technical Centre for Nuclear and Radiation Safety). Interaction between these organizations is described in this chapter as well.

REFERENCES

Anikanov, S., et al (2003). Assurance and safety assessment of safety parameters display systems on NPP units with WWER-1000 reactors. *Nuclear and Radiation Safety,* (1).

Brenman, O., et al. (2006). Licensing review of foreign I&C systems for Ukrainian power plants. In *Proceedings of International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies* (NPIC&HMIT 2006). Albuquerque, NM: NPIC & HMIT.

IEC. (1998). *Functional design criteria for safety parameter display system for nuclear power stations*. IEC.

Kolesov, S., et al. (2000). Safety parameters display system (SPDS) for Ukrainian NPP with WWER-1000 reactor type. In *Proceedings of International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies* (NPIC&HMIT 2000). Washington, DC: NPIC & HMIT.

NP. (2000a). *General regulations of nuclear power plant safety assurance*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2000b). *Requirements for nuclear and radiation safety of information and control systems important to the safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Committee.

USNRC. (1981). *Functional criteria for emergency response facilities*. Washington, DC: U.S. Nuclear Regulatory Commission.

ADDITIONAL READING

Fleger, S., et al. (2010). *Updating the NRC'S Human Factors Engineering Design Review Guidance* / International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2010), Las Vegas, Nevada.

Ji, S., et al. (2012). *Development of Technical Improvements for CPR1000 Advanced Main Control Room in China* / International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2012), San Diego, California.

NRC. (2002). *NUREG-0700 Rev.2. Human-System Interface Design Review Guidelines*. U.S. Nuclear Regulatory Commission.

NRC. (2004). *NUREG-0711 Rev. 2. Human Factors Engineering Program Review Model*. U.S. Nuclear Regulatory Commission.

Schultz, E. E., et al. *User interface design in safety parameter display systems: direction for enhancement* / Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants, Lawrence Livermore Nat. Lab., California Univ., CA.

Seong, N. C., et al. (2012*). The Regulatory Experiences and Activities of Human Factors Engineering at Korea Nuclear Power Plants* / International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2012), San Diego, California.

Seong-nam, C. et al. (1993). *Technical report for the implementation plan of the Safety Parameter Display System in operating NPPs (KINS/AR-167)*. Daejeon: Korea Institute of Nuclear Safety.

USNRC. (1981). NUREG-0835. *Human Factors Acceptance Criteria for the Safety Parameter Display System*, U.S. Nuclear Regulatory Commission. *The Carta Vita Safety parameters display systems*, from http://www.kfki.hu/~aekihp/arlhome/certadoc.html.

USNRC. (1986). *Safety parameter display system. Malfunctions*, from http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1986/in86010.html.

Woods, D. D., et al. *Evaluation of safety-parameter display concepts, volume 2* from http://adsabs.harvard.edu/abs/1982wec.

KEY TERMS AND DEFINITIONS

Main Control Room: An information and activation center of NPP for the operators in normal operation, anticipated operational occurrence, design basic accidents and severe accidents.

Safety Function: A specific objective that has to be fulfilled for safety assurance.

Safety Limits: Limits on operational parameters within which an authorized facility is shown to be safe.

Safety Parameters: Main parameters associated with safety functions (e.g. for safety function "reactivity control" – reactor power, reactor period, control rod position, boric acid concentration).

Safety Parameters Display Systems: A system for assistance to the operator in quickly determination of deviations in NPP unit operation.

Software-Hardware Complex: An aggregate of hardware, software and service apparatus central part of I&C systems, which are delivered to NPPs as full assembly after checkout and testing with high level of factory availability.

Chapter 12
Organization and Information Support of Expert Reviews of I&C Systems Modernization at NPP of Ukraine

Alexander Klevtsov
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

Vladislav Inyushev
State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine

ABSTRACT

Safety assessment of Instrumentation and Control systems (I&C systems) of NPP is performed during expert reviews of nuclear and radiation safety in the framework of the licensing process at all life cycle stages of I&C systems. Life cycle stages of NPP I&C systems, which are determined by current guides, rules, and standards of Ukraine, are considered in the chapter. A short overview of the main principles of safety regulation of nuclear facilities, licensing, and expert review of nuclear and radiation safety is presented. Specific safety assessments of NPP I&C systems at different life cycle stages are analyzed (in particular, a list of documents proving NPP I&C safety that should be submitted for expert review at each stage is given). Such assessment is a labor-intensive process that requires processing considerable amounts of a variety of information. Hence, it is reasonable to provide experts with information support for assessing the safety of NPP I&C systems. The chapter gives suggestions and examples of practical implementation of the automated system for support of expert activities and considers the knowledge base for I&C systems.

INTRODUCTION

Safety assurance is one of the most important tasks during the operation of nuclear power plants. Instrumentation and control systems play an important role and are involved in control of a majority of technological processes at NPPs.

Life cycle of the NPP I&C systems consists of several consecutive stages that cover development of systems requirements, design, testing, implementation in NPP, operation. Furthermore, assessment of the NPP I&C systems is performed at all life cycle stages in the framework of expert review nuclear and radiation safety (NRS).

DOI: 10.4018/978-1-4666-5133-3.ch012

Expert review of the NPP I&C systems requires effective information support because of processing of a large amount of different information. In the field of the I&C systems it is especially significant due to the following reasons:

1. Each I&C system sometimes contains tens of thousands electronic components;
2. At present a process of rapid development of electronics and computer technology both in hardware components and software is taking place, it causes a necessity for modernization of the NPP I&C systems not only because of their physical ageing but also of obsolescence (while NPP technological equipment does not undergo such changes);
3. Due to the fast development of electronics, normative base in the field of the I&C systems is also improving quickly enough.

Hence, experts have not only to analyze large amounts of information, but also constantly monitor changes of electronics and computer equipment themselves and requirements specified by national and international standards.

This fact necessitates the creation of automated system for support of expert activity for safety assessment of the NPP I&C systems.

The creation of such an information support system can be considered as one of the directions of knowledge management in expert organization. Knowledge management consists in a complex, systematic approach to identification, management and distribution of organization's knowledge and ability of employees to create new knowledge collectively and in such a way to facilitate purpose achievement of this organization. This promotes conditions for improving the work efficiency for all employees at the enterprise by simultaneous decrease of efforts.

BACKGROUND

Expert reviews of modernized I&C systems for NPP of Ukraine are performed according to requirements of national regulatory documents (NP, 2005,a, GND, 2000, NP, 2005,b, NP, 2000), and recommendation of international standards IAEA, 2002, IEC, 2011 and other.

At present the procedure of NPP I&C systems expert review is not automated in Ukraine. Earlier some scientists issued different publications (e.g. Khvastunov, 1981, Bashlykov, 1986, Tokarenko, 2000, Larichev, 2008), about using of expert assessments and designing of making-decision systems in power engineering. But these publications describe only technological processes and operative-dispatch management and were based on comparison of separate decisions of different experts. This does not take place in our case, because decisions are made by a group of experts and are not disputed.

Scientists Konorev, 2007, Kharchenko, 2004 solved the task of automation of software analysis and assessment of NPP I&C systems and development instrumentation tools for this work. But this task covers only part of expert reviews for NPP I&C systems.

This chapter contains a short overview of expert review organization at different life cycle stages during NPP I&C systems modernization. Proposals for automation of NPP I&C systems expert review process through creation of an automated system for information support of expert activity are made in the chapter.

SAFETY LIFE CYCLE OF THE NPP I&C SYSTEMS DURING THE MODERNIZATION

There is a large number of life cycle models (further – LC) of I&C systems, describing in various international (for example, in IAEA, 2002, IEC, 2008, IEC, 2011, ISO/IEC, 2008) and national (for example, in GOST, 1992,b, DSTU, 1999, USNRC, 2010) regulatory documents. At the moment, one of the most known models for NPP I&C systems is V-model of LC (IAEA, 2002).

It should be mentioned that in Ukraine in most cases the point is not in the implementation of fundamentally new I&C systems or systems on new power units (such cases are relatively uncommon), but in general about modernization of current, obsolete and physically ageing NPP I&C systems. Therefore one of the main regulatory documents that define LC stages of I&C systems is NP 306.2.106 "Requirements for modification of nuclear plants and procedure for their safety assessment."

According to NP, 2005,b, when changes occur in the design, structure of safety important systems (including I&C systems), or their characteristics and software, the operator develops and agrees technical decisions for specified stages of modification with the regulatory authority.

So, LC stages of the NPP I&C systems are connected with making proper technical decisions by the operator or with releasing other documents, substantiating safety of the NPP I&C systems (requirement specification, engineering design etc.). Technical decisions are approved by operator management, agreed with the design organization (as required), and submitted to the regulatory authority for approval. Each next stage of modification at NPP can be started only after approval of a proper technical decision. The operator should provide required documentation sufficient for consideration and assessment of a proper technical decision by the regulatory authority in time.

On the basis of the analysis NP, 2005,b six main life cycle stages of the NPP I&C system can be marked out:

- Development of a modification concept of the NPP I&C system (or implementation of the new NPP I&C system);
- Development of technical requirements for modernization (creation) of the NPP I&C system;
- Design, production and testing of components of the I&C system at the enterprise;
- Assembling and commissioning of the I&C system at NPP;
- Putting the i&c system into trial operation at npp;
- Putting the I&C system into stationary operation at NPP.

Each life cycle stage is conformed to a specific set of documents released by the I&C developer, design organization or NPP for safety validation of implemented (modified) I&C system.

Let us consider these stages sequentially.

Stage 1: Development of modification concept of the NPP I&C systems (or implementation of the new NPP I&C).

At this stage, the operator develops a conceptual decision of NPP modification that is agreed by the regulatory authority before starting any operations related to NPP modification.

The conceptual decision should contain the following information:

- Determination of the modification object;
- Purpose of modification, substantiation of its necessity with determination of safety deficiencies or deviations from requirements of safety standards and rules, which are eliminated by the suggested modification;
- Short description of modification;
- Assessment of modification effects on safety of NPP, its personnel and environment;
- Suggestions regarding determination of safety class and classification indicator of the modification object;

- Possibility and suitability of preservation of individual elements of the modified object, taking into account their technical condition and compliance with requirements of standards and rules of NRS;
- Other (besides effects on safety) expected technical and economic modification results;
- A list of participants of modification (designers, suppliers of equipment and services, software designers etc.);
- Results of operation of similar modification objects on other NPPs (if it is possible);
- Time schedule to implement modification with determination of required modes of tests.

If necessary, after consideration of conceptual technical decisions the regulatory authority develops a plan of safety assessment of modification project, in which LC stages of NPP I&C systems, documents released at each stage and expert reviews (see below) of these documents are provided.

Stage 2: Development of technical specifications for creation (modernization) of the NPP I&C systems.

Initial data and requirements on system are specified by the customer (operator) taking into account the I&C system purpose, its connections with other systems, peculiarities of operating personnel work, results of analysis of power unit safety. These requirements should not depend on possible ways of system implementation. For a new or modernized system initial data and requirements define at least:

- Purpose, main and additional functions and their role in safety assurance;
- Lists of controlled parameters, events and states;
- A variation range and limits of probable values of controlled parameters;
- Dependencies between inputs and outputs of each function specified in a form of verbal descriptions, formulas, tables, and algorithms;
- Requirements on accuracy, time characteristics, dependability (reliability and maintainability) of each of basic functions;
- Signals, interfaces and protocols of data communication with other instrumentation and control systems.

Expected conditions in the estimated places of equipment installation are also specified: operating and limit values of influencing factors of environment and specific environments (if any), mechanical and electrical influences, characteristics of electromagnetic environment, possible long- and short-term deviations of power supply parameters, within which equipment should perform its functions with required quality and reliability.

Initial data determined by the customer and requirements to the system are concretized and supplemented in requirement specification (RS) for creation or modernization of the I&C systems.

Requirement Specification:

- Defines the system structure and distribution of functions among its components (subsystems);
- Regulates initial data and requirements on components (hardware, software and software-hardware complex (SHC)) that should be developed for the system (detail definition of term “software-hardware complex” is given in Chapter 1);
- Defines a list of earlier developed (“ready”) components, which are supposed to be used in the system, determines requirements on such components and also a necessity, volume and ways of checking compliance with these requirements (qualification).

In requirement specification for creation (modernization) of the I&C systems requirements on personnel, premises, quality of primary power supply, organizational protective actions against unauthorized access, tests, acceptance and maintenance of the system on the operating site and others can be also specified. Quite often modification covers not the I&C system as in whole, but only some of its part. In this case RS can be issued for development and implementation of only this part, e.g.: core (i.e. SHC), separate hardware and software.

In specification requirement for development, production and delivery of the SHC, at least, the following requirements are regulated:

- For the main and additional functions;
- For reliability, tolerance, quality, independence of performed functions;
- For software and dataware;
- For safety substantiating documents;
- For development and production quality assurance;
- For assessment and justification of compliance at all stages of life cycle.

For each of the performed functions the following are specified in RS: purpose; a list of controlled parameters, events and conditions; variation ranges and limits of probable values of controlled parameters; types of input and output signals; relation between inputs and outputs (in the form of formulas, tables or algorithms); other data required and sufficient for performance of the function. In RS a reserve of equipment and computer power of the SHC required for provision of a possibility for system modernization, when functional requirements change (extend) at further life cycle stages, and also for compensation of occurred faults if the replacement of failed element is temporarily impossible or unreasonable, is usually provided. For all independently operating parts of the SHC requirements of tolerance or resistance to external influences (environmental, mechanical, electric, electromagnetic) in operation and extreme conditions are regulated.

In RS on the SHC requirements on production, factory tests and acceptance, marking, packaging, transportation and storage of components, manufacturer's guarantees and other typical for manufacturing production should be determined.

Stage 3: Design, production and testing of the I&C components at the enterprise.

At this stage, as the level of detail increases, the assessment of obtained results is performed. During this stage required changes can be made in earlier approved technical decisions until stepwise approximations will achieve system configuration, satisfying standards and rules of NRS, initial data and customer's requirements and RS requirements on system creation (modernization). After the design process achieves such a detail level, when it is known how the specified functions will be performed, what new (developed specially for the designed system), replicated and industrial components will be applied and how these components should be configured, project documentation, including ordered specifications on equipment procurement, is issued.

During the process of the SHC development a composition, structure and distribution of functions among its components are determined; possibility and reasonability of the use of earlier developed hardware are assessed; make a solution about the use of borrowed (replicated) and commercial items; chose elemental and constructive base for new components that should be developed for the SHC. Made technical decisions can be corrected at further stages, taking into account technical and economic reasonability and on the basis of assessment of their compliance with requirements of regulatory documents and RS. Software of the SHC is developed and verification is performed at all stages of their creation – during formulation of initial data, design, coding, integration with hardware. According to NP, 2005,b, NP, 2000 plan and report on software verification are submitted for approval to the regulatory authority in a package of documents of technical decision on assembling of the NPP I&C systems (see below Stage 4).

At the final development stage design and software documentation that defines composition and structure of the SHC and contains required data for its production, checking (control, testing) and acceptance is released.

During validation compliance of the developed SHC to requirements of guides and rules of nuclear and radiation safety and RS is made. Validation is performed by development organization and manufacturer of the SHC according to the validation plan agreed with the regulatory authority. The first stage of validation is preliminary off-line tests of components and complex tests of the SHC with simulators of signal sources and receivers. At the second stage acceptance testing of the SHC, in which designers, manufacturers, representatives of prospective customers and regulatory authority are participating, are performed. Validation results reflected in a proper report, act and protocols of preliminary and acceptance testing are submitted for control to the regulatory authority. Positive results of validation are the basis for shipping the SHC to NPP.

Stage 4: Assembling and commissioning of I&C systems at NPP.

At this stage, the operator develops a technical decision on assembling of the modification object including the following activities: disassembling (if necessary) of old equipment, assembling of new one, commissioning, preliminary (off-line and complex within the NPP) testing of the modification object.

To substantiate possibilities to carry out these activities the operator attaches the following documents to technical decision on assembling of modification object:

- Requirement specification for modification object agreed according to the established procedure with the regulatory authority;
- Preliminary safety analysis report of modification project of NPP;
- Program and methods of preliminary testing of modification object (off-line and complex within NPP);
- Quality assurance program of modification;
- Software verification plan and verification report;
- Results of the SHC validation (if the SHC is modified);
- Materials of algorithms' verification which were changed during modification.

During the I&C system modification the following documents within safety analysis report or in the form of separate documents are additionally attached:

- Design assessment of I&C system reliability;
- Analysis of system response to probable failures in it;
- Stability analysis of control and regulation loops (if any).

At this LC stage preliminary complex testing of the system is performed at NPP for confirmation that each of the functions specified in RS is performed with the required quality and reliability. Final approval of compliance of the I&C systems to requirements of guides, rules, and standards on nuclear and radiation safety and RS is performed at further stages during trial operation and acceptance testing of the system.

Stage 5: Putting the I&C systems into trial operation at NPP.

According to Yastrebenetsky, 2012 all I&C modernizations can be divided into pilot (modernizations implemented for the first time at NPP with specific reactor type) and replicated (modernizations implemented before at a specific NPP type in Ukraine and showed positive results). Of course, use of replicated systems is preferable in terms of safety justification and cost for acquisition of systems. The scope of licensing actions for replicated modernizations is substantially smaller than for pilots. A specific stage in the implementation of a pilot system is its trial operation with extensive support from the designer and prompt feedback from the NPP to the designer, involving analysis of all failures, faults or NPP personnel comments.

At this stage operator develops technical decision on putting of the modification object into trial operation.

According to GOST, 1992,a trial operation is performed to define actual knowledge of quantitative and qualitative characteristics of the I&C systems and personnel readiness to work in operation conditions of the I&C systems, to define actual I&C systems efficiency and for documentation correction (if necessary).

To substantiate the safety under putting of the modification object into trial operation the following documents are attached to technical decision:

- Report or other documents (act, protocols) containing results of assembling and commissioning;
- Report on results of preliminary complex testing of modification object within NPP, submitting protocols and acts of testing execution;
- Information about results of metrological test of measuring lines (if any);
- Information about personnel training involved into modification object operation;
- Information about applied temporary changes into design and operational documentation;
- Program of trial operation of modification object;
- Program and methods of acceptance testing of modification object (can be submitted later, but under the condition of approval by the beginning of acceptance testing).

According to results of trial operation a decision of possibility of submission parts of the I&C systems and the system in a whole for acceptance testing is made. The work is finished with drawing up an act of completion of trial operation and system allowance for acceptance testing.

Stage 6: Putting of I&C systems into stationary operation at NPP.

After successful completion of trial operation, a technical decision on putting of the modification object into stationary operation is developed for implementation and a task for putting modification object into stationary operation as a part of NPP is agreed with the regulatory authority.

To substantiate the safety under putting modification object into stationary operati at NPP, attach the following documents to technical decision:

- Report or other documents (act, protocols) containing results of trial operation;
- Act and protocols of acceptance testing and other materials of interauthority acceptance commission;
- Final safety analysis report improved according to results of trial operation;
- Information about application of changes into design and operational documentation;
- Information about results of metrological certification of measuring tools (if required).

PRINCIPLES OF SAFETY ASSESSMENT OF THE MODERNIZED NPP I&C SYSTEMS IN UKRAINE

According to Law of Ukraine "On Nuclear Energy Use and Radiation Safety" (Law of Ukraine, 1995) during development and implementation (modification) of NPP safety important I&C systems at all LC stages the assessment of their safety, performed by expert authorities during State expert review of NRS in the framework of scientific technical support of the regulatory authority is mandatory.

Thus, all documents substantiating safety of the NPP I&C systems undergo expert review of State expert review of NRS. In case of a positive result of expert review of documentation, issued at a specific life cycle stage, the regulatory authority gives a permit to proceed to the next stage of the project for development and implementation of I&C systems at NPP.

NPP nuclear and radiation safety is a feature of not exceeding determined limits of radiation effect on personnel, population and environment under normal NPP operation, failures of normal operation and design basis accidents and also of restricting radiation effects under beyond design basis accidents. NPP I&C safety is understood as a part of NRS, which relates to jointly operating I&C systems and technological equipment of NPP power units and depends on proper operation of the I&C systems.

Safety regulation of nuclear energy use is performed by specially established regulatory authority and is one of the fundamental principles of safety management, which purpose is safety assurance for people, natural environment, NPP and sources of ionizing radiation. State regulation of safety of nuclear energy use includes:

- **Standardization:** Determination of national regulatory criteria and requirements, defining conditions of use of NPP and sources of ionizing radiation,
- **Licensing:** Authorization for performing activities connected with use of NPP and sources of ionizing radiation;
- **Inspection:** Execution of inspection for compliance with the requirements and conditions of provided permissions by organizations and enterprises using NPP and sources of ionizing radiation.

The regulatory authority acts independently from designers, constructors, operators to such an extent that is required for safety assurance was the only task of personnel of this authority. For efficient performance of its functions, the regulatory authority possess all required legal powers, has a full access to NPP and to proper information which is held by operator.

Let us consider in detail a function of the regulatory authority such as licensing (authorization). According to Law of Ukraine "On Authorizing Activity in Nuclear Energy Use" (Law of Ukraine, 2000), authorization activity is a component of nuclear safety regulation. It provides:

- Licensing of activity of operator at separate stages of NPP life cycle;
- Granting of individual permissions on execution of certain types of work or operations at stages of commissioning, operation and decommissioning;
- Licensing of activity connected with direct personnel control of NPP reactor unit;
- Certification of sources of ionizing radiation and elements, safety important for NPP.

The purpose of authorization-based activity is the following:

- Provision of use of NPP only with approved level of safety according to national requirements;
- Provision of activities in the field of nuclear energy use only by those physical and legal

parties that can guarantee performance of requirements of legislation, guides, rules and standards of NRS.

Main principle of authorization-based activity in the field of nuclear energy use is a priority of NRS assurance over other purposes.

Receiving a license by the applicant is the basis to start activities, execution of work and operations connected with certain life cycle stage of NPP. The license determines conditions and limits of such activity performance.

An integral part of licensing process is the assessment in the framework of state expert review of NRS.

In NP, 2005, a concept "state expert review of nuclear and radiation safety" is defined as a complex of organizational, scientific technical and expert and analytical activities that is performed by a special regulatory authority for independent assessment of technical safety level in the field of nuclear energy use, taking into account all factors that lead to nuclear and radiation danger to human health and environment including physical protection assurance.

In Ukraine state expert review of NRS is performed by the State Scientific and Technical Centre for Nuclear and Radiation Safety (SSTC NRS) which is an organization of technical support of the regulatory authority.

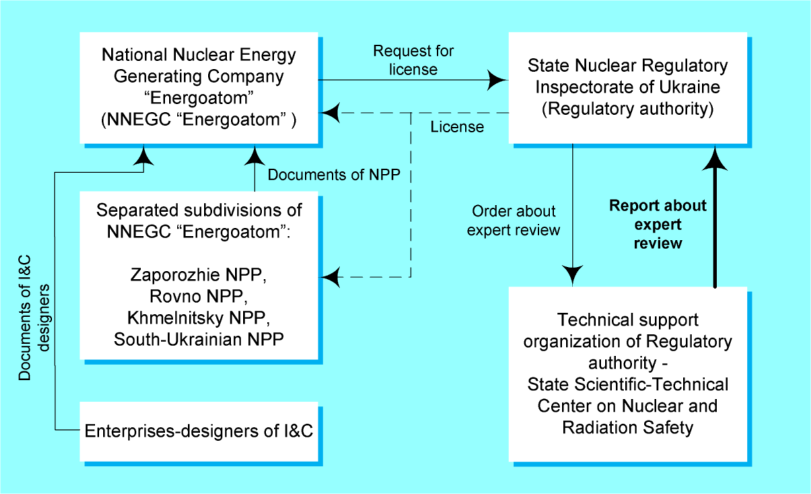
Figure 1 shows a diagram of interaction between different authorities during licensing process (including state expert review of NRS).

State expert review of NRS during modernization of the NPP I&C systems consists in assessment of documentation, substantiating safety of NPP I&C systems for compliance with NPP safety principles and also to main requirements of NRS assurance determined in legislative and regulatory documents currently in force.

In general case an expert review object can be NPP in a whole or its different systems, including components. In particular these objects are new/modernized NPP I&C systems and their components: software-hardware complexes (SHC); hardware (HW); software (SW).

Expert review subject (reviewed documentation) can be design, engineering, technological, software, organizational management and other documents related to expert review object and

Figure 1. Interaction between authorities during licensing process


National Nuclear Energy Generating Company "Energoatom" (NNEGC "Energoatom")
Request for license
State Nuclear Regulatory Inspectorate of Ukraine (Regulatory authority)
License
Documents of NPP
Separated subdivisions of NNEGC "Energoatom":
Zaporozhie NPP, Rovno NPP, Khmelnitsky NPP, South-Ukrainian NPP
Order about expert review
Report about expert review
Documents of I&C designers
Technical support organization of Regulatory authority - State Scientific-Technical Center on Nuclear and Radiation Safety
Enterprises-designers of I&C

containing required data on the basis of which expert review is made.

Expert review purpose is the assessment of coverage and sufficiency of documents, substantiating NRS during the use of NPP from the point of possibility of granting a proper permission (license).

Main tasks of the expert review are as follows:

- Assessment of provisions of reviewed documentation for compliance with purposes and criteria of safety and also main principles of NRS assurance determined by legislative and regulatory documents currently in force;
- Analysis of a nature of suggested organizational and technical measures directed to NRS assurance and also their scope and coverage of compliance with regulatory documents' requirements;
- Reports development of state expert review execution, containing grounded assessment of coverage and sufficiency of substantiation of expert review object safety in reviewed documentation.

According to Yastrebenetsky, 2002,b, Yastrebenetsky, 2001,f procedure of safety assessment during licensing of modernization (reconstruction, creation) activities of the I&C system is based on the following premises:

- Safety assessment is performed during the state expert review executed by the specialized expert organization authorized by the regulatory authority;
- Expert review is executed in separate stages connected with system life cycle stages;
- Assessment results (experts comments with their substantiations, conclusions and recommendations) are given in the report of NRS state expert review that expert organization sends to the regulatory authority after completion of expert review of documentation, which substantiate safety of the NPP I&C systems at current LC stage;
- On the basis of received report, the regulatory authority issues a conclusion of possibility and conditions of document approval, substantiating safety, or technical decision of operator of performing next stage of activities. As a submitting condition it is necessary to incorporate all comments given in the report ("incorporation of comments" is intended to bring the expert review object and/or subject into compliance with specified safety requirements or develop measures required for compensation of detected discrepancies);
- Licensing process can be terminated in a case if a conclusion of the regulatory authority contains a final rejection of approval of the submitted document;
- In case of successful passing of all the expert review stages provided in the licensing plan and if comments provided in the released reports are incorporated, the regulatory authority agrees NPP technical decision on putting of the system into stationary operation.

General diagram of safety assessment of the NPP I&C systems at different LC stages is given in Table 1.

Assessment methods of compliance of the NPP I&C systems with regulatory requirements can be classified in the following way:

- Logical analysis of documents on the verbal level (without any calculations or experimental checking);
- Analysis of documents with checking calculations (e.g. reliability);

Table 1. Safety assessment of modernization (implementation) of the NPP I&C systems at LC stages

LC stage of the NPP I&C systems	Documents substantiating safety of the NPP I&C systems at LC stages	Reports of expert review of the NPP I&C systems
Development of modification concept of the NPP I&C systems (or implementation of the new NPP I&C systems)	Conceptual technical decision of modernization of the NPP I&C systems	Report of state expert review of NRS of conceptual technical decision of the NPP I&C systems modernization
Development of technical requirements on creation (modernization) of the NPP I&C systems	Requirements specification to (modernization) of the NPP I&C systems	Report of state expert review of NRS of requirements specification for creation (modernization) of the NPP I&C systems
Design, production and testing of I&C systems components on the enterprise	Technical project of the NPP I&C systems	Report of state expert review of NRS of technical project of the NPP I&C systems
	Programs and methods of preliminary testing of I&C systems components	Safety assessment at this stage is not performed
	Act and protocols of preliminary testing of I&C systems components	
	Quality assurance program of modernization of the NPP I&C systems	Safety assessment for these documents is performed in frame of expert review of NRS of technical decision of the NPP I&C systems assembling
	Software verification plan of the NPP I&C systems	
	Software verification report of the NPP I&C systems	
	Validation plan of the I&C systems for the NPP I&C systems assembling	
	Report of design assessment of reliability of the NPP I&C systems	
Assembling and commissioning of the I&C systems at NPP	Technical decision of assembling performance of the NPP I&C systems	Report of state expert review of NRS of technical decision of the NPP I&C systems assembling with a package of documents
	Report of I&C systems validation for the NPP I&C systems assembling	
	Report of failure response analysis of the NPP I&C systems	
	Preliminary safety analysis report of the NPP I&C systems	
	Program and methods of preliminary on-site testing of the I&C systems	
Putting the I&C systems into trial operation at NPP	Technical decision of inputting the modernized NPP I&C systems into trial operation	Report of state expert review of NRS of technical decision for putting of modernized NPP I&C systems into trial operation with a package of documents
	Documents containing results of assembling and commissioning	
	Results of on-site testing of the modernized I&C systems	
	Information about personnel training involved in the NPP I&C systems operation	
	Information about introduction of temporary changes in design and operational documentation of the NPP I&C systems	
	Program of trial operation of the NPP I&C systems	

continued on following page

Table 1. Continued

LC stage of the NPP I&C systems	Documents substantiating safety of the NPP I&C systems at LC stages	Reports of expert review of the NPP I&C systems
Putting the I&C systems into stationary operation at NPP	Technical decision for putting of modernized NPP I&C systems into stationary operation	Report of state expert review of NRS of technical decision for putting of modernized NPP I&C systems into stationary operation with a package of documents
	Report of trial operation results of the NPP I&C systems	
	Act and protocols of acceptance testing of the NPP I&C systems and other materials of acceptance commission activities	
	Final safety analysis report of the NPP I&C systems	
	Information about changes in design and operational documentation of the NPP I&C systems according to results of trial operation	
	Information about metrological certification results of measuring channels of the NPP I&C systems	

- Direct participation of experts in verification, validation, testing and acceptance of components (on enterprise) and/or the system (at NPP);
- Independent verification, validation, checking of separate components.

The first group of methods regulated in the regulatory document GND, 2000 has been the most widely used till now. Recently logical analysis of documents is more often added with checking calculations (provided that experts possess required approved methods and/or computing programs) that increases assessment confidence.

In this book we described only organization of safety assessment during the expert review. More detail description of safety assessment procedure and different assessment methods can be found in many other publications, for example in a series of articles on standardization and safety assessment of the NPP I&C systems (Yastrebenetsky, 2001,a-e, Yastrebenetsky, 2002,a-b, Goldrin, 2001, Kharchenko, 2002) and in other publications (Kharchenko, 2008, Sklyar, 2006, Lindner, 2008, Sergienko, 2008, Konorev, 2010, Miedl, 2010).

INFORMATION SUPPORT OF THE EXPERT REVIEWS OF THE NPP I&C SYSTEMS MODERNIZATION

For information support of the expert review it is reasonable to build a knowledge base that will allow accumulating and systemizing and finding different information which is required for experts to perform safety assessment of the NPP I&C systems. Besides that a knowledge base will provide support for other types of activities, such as the development of regulatory documents, NPP support, research and development, international cooperation, preparation of publications and others.

Necessity in automation of I&C systems expert review is caused by the following factors.

1. In Ukraine a wide-ranging implementation of new and modernization of operated I&C systems at NPP power units is performed (in particular within a period from 1996 to 2012 at NPPs of Ukraine more than 250 of various modernizations and implementations of new I&C systems were realized and also more than 800 expert reviews of the NPP I&C systems) (see Table 2).

Table 2. Expert review of modernized I&C system during 1996-2012

Years	Number of modernized I&C systems	Number of expert reviews	Number of assessed documents, substantiating safety	Number of assessed regulatory requirements
1996-2012	257	826	1112	41558

State expert review of NRS is performed at all life cycle stages of the I&C systems. At the same time checking of the I&C systems for compliance with several tens of safety criteria, i.e. mandatory requirements of modern regulatory documents is performed (during each expert review assessment of compliance with 30-40 requirements of guides, rules and standards of NRS is made).

During safety assessment of the NPP I&C system experts have to deal with a large amount of information that makes expert review a labor-intensive process and increases probability of fault occurrence. In particular, experts should:

- Perform analysis of submitted documents for expert review, which substantiate safety of the NPP I&C system;
- Assess different additional designers' and NPP's documents, in which data about modernization, reconstruction and implementation of new I&C system at NPP units of Ukraine, is contained;
- Consider information about implemented (modernized) I&C system (about its composition, structure, functions, experience of approbation of similar systems etc);
- Analyze reports, expert conclusions and analogous documents that contain results of earlier performed safety assessments of the I&C systems and their components;
- Choose rules and methods of safety assessment regulated in regulatory documents and applied procedures (algorithms, programs, calculation formulas etc.);
- Work with regulatory documents, including:
    - ◦ International safety standards and guidelines;
    - ◦ Intergovernmental and national standards, rules and guides in nuclear power engineering;
    - ◦ Regulatory documents of supplier countries of equipment for NPPs of Ukraine, defining regulatory requirements to expert review objects (I&C systems and their components);
    - ◦ Regulatory documents which are currently in force in Ukraine and contain regulatory requirements on expert review subjects (documents, substantiating safety).
- Assess compliance of I&C system with a large amount of requirements on safety regulated in various regulatory documents;
- Reference to native and foreign publications for additional information that can be important for safety assessment of the NPP I&C systems.

It is obvious that such an approach requires information support of expert activities to decrease efforts and increase expert work efficiency.

Knowledge base that will simplify searching and selection of required for experts information is suggested to be developed.

For knowledge base development the following tasks should be solved:

- Development of general structure of the knowledge base;
- Development of detail structure if all chapters contained in the knowledge base;

- Creation of software shell for knowledge base management that will provide possibility of adding, changing and searching of information;
- Acquisition, analysis, systematization and inputting data into the knowledge base.

Structure, purpose and use of knowledge base will be illustrated as an example of knowledge base on the NPP I&C systems that is created within the development process of information environment of SSTC NRS, according to Beliy, 2008. Main principles of knowledge base creation of the NPP I&C systems and the stages of this activity are reflected in Klevtsov, 2007,a-c.

Technically knowledge base is organized in the form of relational database, containing linked tables, forms, and queries. There is no sense to give a detail structure of database in this book. However, in general within knowledge base seven main chapters used during expert review of the NPP I&C systems (and also during execution of other activities) can be marked out:

Chapter 1: "Standards, rules and guides related to safety of the NPP I&C systems;"
Chapter 2: "Regulatory requirements on the NPP I&C systems and their components;"
Chapter 3: "Reports on expert reviews of NPP I&C systems;"
Chapter 4: "New and modernized I&C systems of NPP power units of Ukraine;"
Chapter 5: "Documents from NPPs and designers of I&C systems;"
Chapter 6: "Methods and procedures of expert review;"
Chapter 7: "Results of safety assessment of the NPP I&C systems and their components."

Besides, four auxiliary chapters, not being directly relevant to preparation of report of safety expert review, but can be useful in providing information support to experts, are included in a knowledge base:

Chapter 8: "Incidents in NPP operation caused by I&C systems;"
Chapter 9: "Terms and definitions;"
Chapter 10: "Reports on research and development activities;"
Chapter 11: "Publications."

Specified topics are outlined in knowledge base nominally. Each such chapter covers a part of knowledge base (tables, queries, and forms) that is related to only one specific topic.

General structure and main directions of the knowledge base at NPP I&C systems are shown in Figure 2.

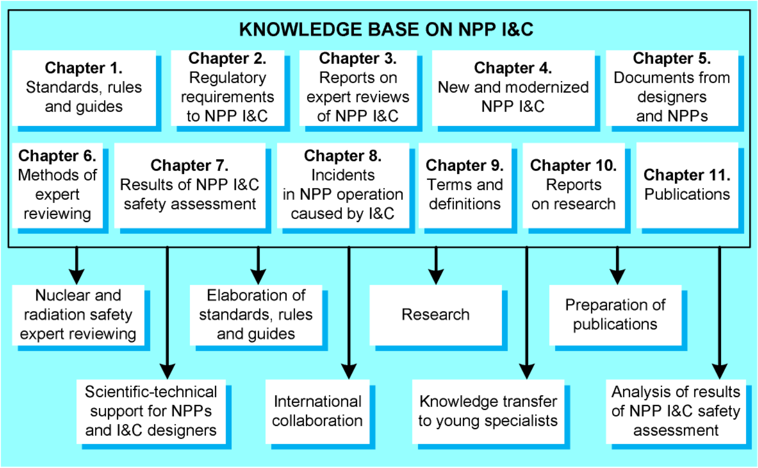
The structure of each of mentioned above chapters is determined taking into account experience of safety standardization and assessment.

Chapter 1 includes regulatory documents related to safety of the NPP I&C systems. The knowledge base contains an identification number of a regulatory document, its name and full text in electronic or printed form. Besides that for each of regulatory documents additional features that allow connecting it (in case of such unambiguous connections) with a certain type of I&C systems, with one or another component of I&C systems (for example, with certain types HW or SW), with system safety class or with life cycle stages, to which this document is related, are determined.

In the knowledge base regulatory documents are classified by organization-developer:

- Standards of the International Atomic Energy Authority (IAEA);
- Standards of the International Electrotechnical Commission (IEC);
- Standards of the International Organization for Standardization (ISO);
- European National Standards;
- USA National Standards, IEEE standards, US NRC documents;
- Intergovernmental standards;
- Guides of State Nuclear Regulatory Inspectorate of Ukraine;

Figure 2. General structure of the knowledge base at NPP I&C systems


KNOWLEDGE BASE ON NPP I&C
Chapter 1. Standards, rules and guides
Chapter 2. Regulatory requirements to NPP I&C
Chapter 3. Reports on expert reviews of NPP I&C
Chapter 4. New and modernized NPP I&C
Chapter 5. Documents from designers and NPPs
Chapter 6. Methods of expert reviewing
Chapter 7. Results of NPP I&C safety assessment
Chapter 8. Incidents in NPP operation caused by I&C
Chapter 9. Terms and definitions
Chapter 10. Reports on research
Chapter 11. Publications
Nuclear and radiation safety expert reviewing
Elaboration of standards, rules and guides
Research
Preparation of publications
Scientific-technical support for NPPs and I&C designers
International collaboration
Knowledge transfer to young specialists
Analysis of results of NPP I&C safety assessment

- National Standards of Ukraine (DSTU);
- State Standards of former USSR (GOST), which are still in force;
- National Standards of Russian Federation, Regulation of Federal Department on ecological, technological and atomic supervision of Russia;
- Company standards of SSTC NRS.

In addition regulatory documents are classified by a considered object according to Yastrebenetsky, 2004:

- Documents directly related (and only) to the NPP I&C systems and/or their components (class A);
- NPP safety documents that contain requirements on different NPP systems and elements, including the NPP I&C systems (class B);
- Documents related to industrial (used in different branches of industry) I&C systems and their components which are also applied at NPP (class C);
- Documents, containing general technical requirements that are also relayed to the NPP I&C systems and their components (class D):
  - Safety in different branches (D1 subclass);
  - Reliability, diagnostics, testing (D2 subclass);
  - Software (D3 subclass);
  - Electromagnetic compatibility (D4 subclass);
  - Quality assurance (D5 subclass);
  - Different (general technical documents important for the NPP I&C systems, but not included in the classes mentioned above) (D6 subclass).

It should be noted that in Chapter 1 and all other chapters of knowledge base selection of required data can be made by a combination of classification features, which are specified for objects considered in a certain chapter.

Chapter 2 contains a set of regulatory requirements, regulated in national and international regulatory documents. This chapter allows performing through review of definitions of the same requirements in different regulatory documents of Ukraine and international ones. All requirements in knowledge base are grouped by types (for example, requirements on reliability, on quality assurance, on resistance to influencing factors etc.). For each of the specified type of requirements there are definitions from different regulatory documents in the knowledge base (full text of requirement with a reference to a proper regulatory document, form which this requirement was taken, is given). Besides that, by analogy with the classification of regulatory documents specified in Chapter 1 of the knowledge base, requirements can also have additional classification features that allow referring them to a certain stage of life cycle, safety class, type of I&C systems or its components.

Due to use of this structure instead of sequential review of a large amount different regulatory documents expert can quickly search of a separate regulatory requirement and view how it is formulated in different standards and guides.

Chapter 3 contains reports of state expert review of NRS, published by SSTC NRS in 1995-2012, and also protocols of incorporation of expert comments and other materials containing results of safety assessment of the I&C systems and their components. The knowledge base contains names, registration numbers, dates of issue, responsible expert review executor and full texts of expert review reports of the NPP I&C systems. Moreover, for each report additional classification features, specifying an object (i.e. name of I&C system, its modernized part, NPP and power unit, on which I&C system is modernized or implemented, enterprise-developer of I&C system or its components) and an expert review object (i.e. a certain document, substantiating safety) are determined.

Chapter 4 contains data of modernized or new I&C systems, implemented at NPPs of Ukraine. The knowledge base includes name of modernized (new) I&C systems, name of enterprise-developer of I&C system, NPP and power unit, on which the I&C system is implemented, its safety class, year of implementation (modernization) and short description of the system and the scope of its modernization.

Chapter 5 contains documentation (in electronic and printed form) NPP and enterprises-developers of modernized NPP I&C systems that was submitted to SSTC NRS for expert review. This information is included to the knowledge base, because it is often used during expert activity for safety assessment of similar I&C systems implementation at NPPs of Ukraine. Possibility of comparative analysis of analogous systems not only increases quality of expert review, but also simplifies expert’s work.

The knowledge base contains title and full text of document and also information about organization-developer of this document. Also for each document additional features are determined. They define to which exactly I&C systems this document is related, for which NPP and power unit was developed.

Moreover, in the knowledge base a connection between documents, substantiating safety (contained in Chapter 5) and expert review reports of these documents (contained in Chapter 3) is established. Also a connection between documents (Chapter 5) and those NPP I&C systems (Chapter 4) to which these documents are related is organized.

Chapter 6 contains native and foreign safety assessment methods. In the knowledge base name of method, organization-developer of this method, title of document, in which this method is described and a full text with description of method are specified.

The knowledge base contains the following methods:

- Methods of logical analysis of documentation;
- Methods of probabilistic safety analysis;
- Methods of design assessment of I&C system reliability;
- Methods of static and dynamic analysis of software of I&C systems.

The methods elaborated and used by different organizations are included in knowledge base:

- IAEA methods;
- Methods of SSTC NRS;
- Methods of the regulatory authority of Russia;
- Methods of European regulatory authorities;
- Methods of the nuclear regulatory authority of USA (US NRC);
- Methods of Institute of Safety Technologies (Germany).

In Chapter 7 results of expert reviews of NRS of the NPP I&C systems are contained. Data about meeting of regulatory requirements in documents, substantiating safety of the NPP I&C systems, which passed expert evaluation, are included in this chapter. Requirements of regulatory documents which was checked during expert reviews of NPP I&C systems, and also assessment of compliance to these requirements are included to the knowledge base.

If a requirement is not sufficiently met in the reviewed document, then one of the three categories of comments is specified:

- **Category I:** Expert review comment is aimed at elimination of probable danger (if an actual failure to meet requirements of NRS in modernized I&C systems is detected);
- **Category II:** Expert review comment is aimed to obtain required proofs in safety assurance (if it is detected that a requirement of NRS is performed in modernized I&C systems, however its compliance is not sufficiently described in document substantiating safety);
- **Category III:** Expert review comment is aimed to improve document quality submitted for expert review (if inaccuracies of formulations, contradictions, misprints etc. are detected in a document substantiating safety).

For convenience of data search and processing a possibility to search by a random combination of such classification features as NPP name, power unit number, name of I&C systems, enterprise-developer of I&C system, type of document which substantiates safety, number of expert review report and title of regulatory requirement, is provided in this chapter.

On the basis of these data a statistic analysis that allows detecting different adverse tendencies, to which expert should pay special attention during safety assessment in future, will be performed. Purposes of this analysis are as follows:

1. Detection of most problematic requirements, compliance with which is the worst specified in documents substantiating safety;
2. Detection of the most problematic systems from the point of compliance with regulatory requirement of NRS;
3. Detection of designers that issue documents of the lowest quality (i.e. with the largest amount of expert comments on them);
4. Detection of systems and specified to them requirements for which the most severe and important comments during expert review due to discrepancies significantly effecting safety;
5. Possible detection of other adverse peculiarities and tendencies that should be taken into account during expert review of NRS.

Chapter 8 contains information about incidents in NPP of Ukraine caused by failures (disoperation or false operation) of I&C systems. For each incident name, date and time of occurrence, detail description, causes of incident and its category according to international scale of INES (that specifies evaluation of incident from the point of influence to NPP safety) is specified. As additional classification features for convenient data search the following are specified: NPP name, number of power unit and I&C system that caused failure.

In Chapter 9 a set of main terms and definitions of SSTC NRS (according to national and international regulatory documents), used during safety assessment and analysis of the NPP I&C systems and during development of regulatory documents, is included. Its necessity is caused by that one and the same terms can have different definition in different regulatory documents of Ukraine and international standards. For convenient search all terms are divided into specific enlarged groups, for example, terms related to NPPs, to their safety, to quality assurance, to reliability etc.

Chapter 10 contains reports of research and development activities related to NPP I&C systems and performed by employees of SSTC NRS. In the knowledge base title of report, author's name, date of issue and text of report are contained.

Chapter 11 contains publications of employees from SSTC NRS and other Ukrainian and foreign authors classified in the following way:

- Safety and risk;
- Reliability;
- Related issues.

Each of these categories is divided into three subcategories:

- General issues;
- NPP;
- Other branches.

In turn, each of them is divided into two subcategories:

- I&C systems;
- Issues not related to I&C systems.

For each publication a title, author, edition (magazine, collected papers), in which the article is published, year of publication, publishing house and full text are specified.

Note that Chapters 1-7 are devoted to direct use during expert review of NRS. At the same time, other Chapters 8-11 are auxiliary and provide a possibility to obtain additional information, that can be required for experts during safety assessment of the NPP I&C systems.

When it's necessary in future, a considered list can be extended, and new chapters can be additionally included into the knowledge base according to specific organization's needs.

The described above knowledge base can be the basis for creation of automated system for support of expert activity (ASSEA). First steps for development of knowledge base and ASSEA in SSTC NRS was described in Klevtsov, 2007,a-c, Klevtsov, 2008, a-b.

The purpose of such work is development of software that will allow efficiently accumulating, systemizing, processing and quickly finding required data contained in different information sources for supporting NRS expert review of the NPP I&C systems.

The knowledge base is a main component of the ASSEA that allows experts to apply knowledge bases and retrieve information required for making decisions during expert review of the NPP I&C systems.

It is supposed that the ASSEA will include the following elements:

- Subsystem of making-decision support;
- Knowledge base;

- Knowledge base editing subsystem;
- Interface subsystem;
- Reference subsystem.

Software of the ASSEA is a complex of low level tools to work with each separate database including in the knowledge base on the NPP I&C systems. Furthermore, software of the ASSEA includes high level tools to work with the knowledge base in a whole and to run low level utilities.

Software shell of the ASSEA should provide possibility both to perform centralized search of required information in the whole knowledge base and operations separately with each specific chapters of the knowledge base. It is also supposed that the ASSEA should allow not only performing navigation and search of required information in the knowledge base, but also provide automation of some standard procedures that are currently, in fact, are performed by experts "manually":

- Selection of required regulatory documents (from Chapter 1 "Standards, rules and guides") by a specified type of I&C system and document;
- Selection of analyzed regulatory requirements (from Chapter 2 "Regulatory requirements") by a specified type of I&C system and document;
- Selection of earlier executed expert reviews (from Chapter 3 "Reports of NRS expert reviews") by a specified I&C system;
- Selection of systems information (from chapter 4 "new and modernized npp i&c systems") by a specified I&C system;
- Selection of documents of enterprise-designer and NPP related to the system (from Chapter 5 "Documents from designers and NPP") by a specified I&C system;
- Selection of document assessment and analysis methods (from Chapter 6 "Methods of expert review") by a specified type of reviewed document;
- Obtaining of statistical data by results of earlier executed expert reviews (form Chapter 7 "Results of NRS expert review of the NPP I&C systems") for a specified type of I&C system and document substantiating safety;
- Composition of preliminary sample of future report of expert review on the basis of selected information.

All complex of considered tools and databases is a fully functional software product for management and use of the knowledge base on the NPP I&C systems during expert and research and development activities.

Subsystem of making-decision support includes the following modules.

1. Module of forming of regulatory profile.

This module according to a specified type of I&C system and document, substantiating safety, allows performing automated selection of regulatory documents and regulatory requirements, compliance with which is assessed during the expert review of NPP I&C system.

2. Module of documents circulation.

This module allows keeping records of all documents related to expert review of NPP I&C systems. Due to this module consecutive recording of incoming documents (letters, documents submitted for expert review, additional documents, inquires etc.), internal documents (order of expert review implementation, records of expert council meeting), contract documentation and outgoing documents (letters, reports, records on incorporation of review comments, draft conclusions on expert review results etc.) is provided.

3. Module of find of information.

Module is devoted to provide a user with a possibility of information search by a random combination of classification features, specified in each chapter of the knowledge base, and also for full-text search by specified key words or phrases.

4. Module of users authorization.

This module serves for authorization of employees using the ASSEA and knowledge base to provide a possibility of carrying out different activities for different user groups. For all users search and selection of required information from the knowledge base is allowed. Operators of the ASSEA are allowed inputting new information in the knowledge base or modifying its content, using editing subsystem, by adding, changing or deleting records with structure retention. Administrators of the ASSEA (possible involving designers) have a possibility to perform extended systems customization and correction of the knowledge base structure if necessary. Besides that some information can be available only for the specified groups of users (for example, financial and contract documents should be available only for direction of enterprise, head of specific department and workers of accounting department).

A model of structure of the ASSEA is given in Figure 3.

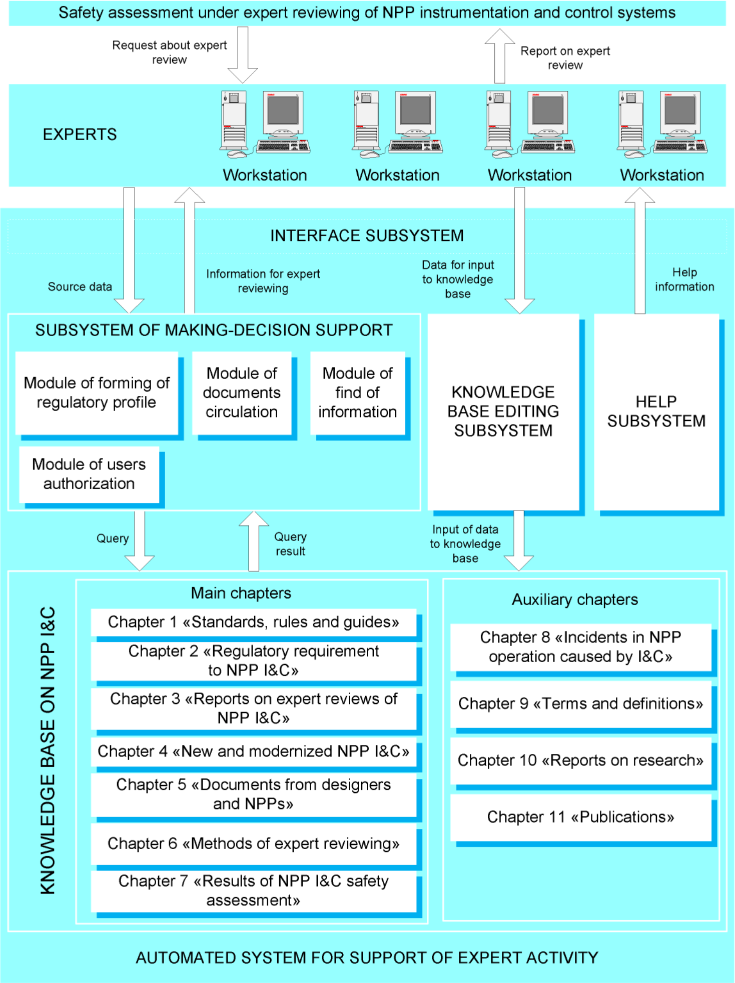
Diagram of application of the knowledge base during safety assessment of the NPP I&C systems under NRS expert reviewing is shown in Figure 4.

Let us explain in more detail way the content of the diagram of formation of report on expert review using the chapters of the knowledge base (see Figure 4).

In the left part of the figure a generalized content of report on expert review is shown. It contains, in particular, the following main components.

1. A list of standards and guides used for expert assessment. This list can be formed by selecting proper standards from Chapter 1 of the knowledge base depending on a specified type of I&C system and document submitted for review. In turn, a list of regulatory requirements, included into Chapter 2 of the knowledge base, is formed from requirements of standards contained in Chapter 1.
2. A list of requirements on object and subject of expert review. By analogy with the stated above a list of regulatory requirements can be also automatically formed on the basis of requirements selection from Chapter 2 of the knowledge base depending on a specified type of I&C system and document submitted for review. In this list both mandatory requirements of national regulatory documents and recommended requirements of international standards are included.
3. Information about earlier expert reviews. A list of expert reviews completed at previous life cycle stages of specific I&C system, implemented on a certain NPP power unit, can be formed on the basis of information contained in Chapter 3 of the knowledge base.
4. Information about operating NPP I&C system. Description of a considered system (or similar system) can be obtained from Chapter 4 of the knowledge base. If the specified I&C system is fundamentally new and there is no information about it, then during an expert review information about this I&C system is input in the knowledge base from submitted documents substantiating safety.
5. Information about requirements on NRS that are declared in a submitted document for expert review. Documents that should be approved by the regulatory authority at a certain life cycle stage of I&C systems are submitted for expert review. Besides that, during expert review different additional documents, substantiating safety, can be

Figure 3. Structure of the automated system for support of expert activity

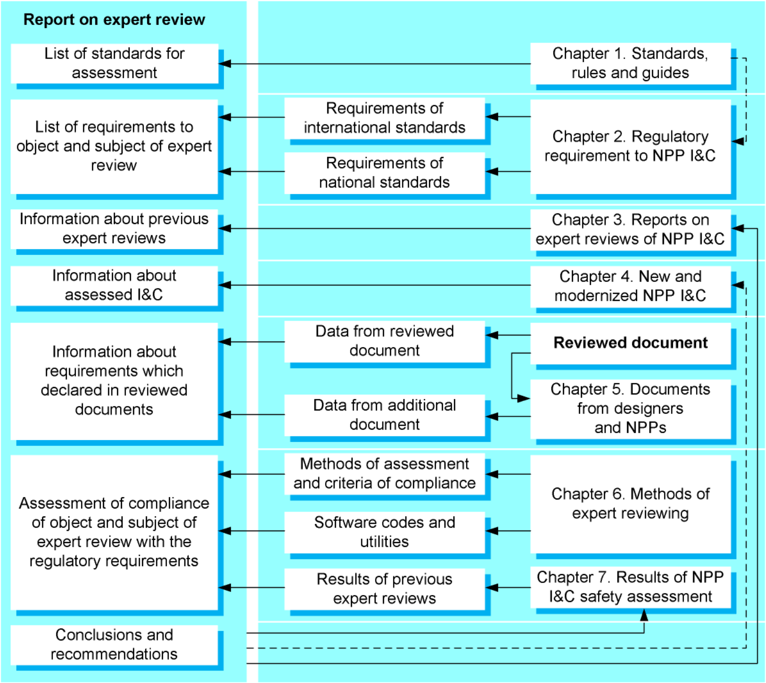

Safety assessment under expert reviewing of NPP instrumentation and control systems
Request about expert review
Report on expert review
EXPERTS
Workstation
Workstation
Workstation
Workstation
INTERFACE SUBSYSTEM
Source data
Information for expert reviewing
Data for input to knowledge base
Help information
SUBSYSTEM OF MAKING-DECISION SUPPORT
Module of forming of regulatory profile
Module of documents circulation
Module of find of information
Module of users authorization
KNOWLEDGE BASE EDITING SUBSYSTEM
HELP SUBSYSTEM
Query
Query result
Input of data to knowledge base
KNOWLEDGE BASE ON NPP I&C
Main chapters
Chapter 1 «Standards, rules and guides»
Chapter 2 «Regulatory requirement to NPP I&C»
Chapter 3 «Reports on expert reviews of NPP I&C»
Chapter 4 «New and modernized NPP I&C»
Chapter 5 «Documents from designers and NPPs»
Chapter 6 «Methods of expert reviewing»
Chapter 7 «Results of NPP I&C safety assessment»
Auxiliary chapters
Chapter 8 «Incidents in NPP operation caused by I&C»
Chapter 9 «Terms and definitions»
Chapter 10 «Reports on research»
Chapter 11 «Publications»
AUTOMATED SYSTEM FOR SUPPORT OF EXPERT ACTIVITY

considered. A part of such documents can be input into the knowledge base at earlier life cycle stages, and newly incoming documents are also input in the knowledge base. Using submitted and additional documents from Chapter 5 of the knowledge base, expert forms a list of requirements on NRS that are declared in the considered documents.

6. Assessment of compliance a documents substantiating safety with the requirements of guides. Using methods, contained in Chapter 6 of the knowledge base, expert assess a level of compliance of requirements, specified in submitted documents for expert review, to requirements of guides, rules and standards on NRS. Besides, according to existing practice methods of documentation analysis are mainly used. However, in a number of cases calculations methods with use of specific software (for example, software for calculation of reliability factors or tools for static and dynamic software analysis) can be used additionally.

Furthermore, results of earlier executed expert reviews, contained in Chapter 7 of the knowledge base, are considered additionally. This is important from the point that during expert evaluations at

Figure 4. Application of the knowledge base during safety assessment of the NPP I&C


Report on expert review
List of standards for assessment
List of requirements to object and subject of expert review
Information about previous expert reviews
Information about assessed I&C
Information about requirements which declared in reviewed documents
Assessment of compliance of object and subject of expert review with the regulatory requirements
Conclusions and recommendations
Requirements of international standards
Requirements of national standards
Data from reviewed document
Data from additional document
Methods of assessment and criteria of compliance
Software codes and utilities
Results of previous expert reviews
Chapter 1. Standards, rules and guides
Chapter 2. Regulatory requirement to NPP I&C
Chapter 3. Reports on expert reviews of NPP I&C
Chapter 4. New and modernized NPP I&C
Reviewed document
Chapter 5. Documents from designers and NPPs
Chapter 6. Methods of expert reviewing
Chapter 7. Results of NPP I&C safety assessment

earlier LC stages comments on the considered system (or documents substantiating safety) that should be incorporated at the current LC stage could be specified. Assessment of incorporation of comments made in previous expert reviews is required for consecutive safety assurance of NPP I&C systems at all LC stages.

In turn, all results of a current expert review are also input into Chapter 7 of the knowledge base to be used at further stages (and possibly for static analysis of expert review results).

7. Conclusions and recommendations. The last chapter of expert review contains short description of main assessment results of submitted documents, comments (if any), conclusions and recommendations to the regulatory authority about possibility of approval of documents or about necessity in their improvement.

Note that the suggested the ASSEA and the knowledge base are devoted to provide only information support of expert review. Direct assessment of compliance of the NPP I&C systems to requirements of guides, rules and standards on NRS cannot be automated and hence is performed by experts.

Finally formed report on expert review is input into Chapter 3 of the knowledge base, and assessment results of performance of separate requirements are input into Chapter 7 of the knowledge base.

Solutions and Recommendations

Expert activity at all life cycle stages of the NPP I&C systems requires effective information support because of large amount of analyzing data during the expert review. Therefore, it is recommended:

- To create knowledge base at NPP I&C systems (set of different information and documents concerning new and modernized NPP I&C systems, including expert review reports);
- To develop automated system for support of expert activity (software shell for effective work with the knowledge base).

FUTURE RESEARCH DIRECTIONS

The future research directions can be as follows:

- Development of safety assessment methods for NPP I&C systems, taking into account requirements of modern national and international standards;
- Improvement of structure and functional subsystems of the automated system for support of expert activity;
- Addition of new information into the knowledge base and its constant updating;
- Provision of similar means for information support in reviews of nuclear and radiation safety not only within NPP I&C systems, but also in other directions (for example, operational safety, neutron physical processes, radiation safety, strength and reliability of NPP structures etc.).

CONCLUSION

NPP instrumentation and control systems pass several life cycle stages from elaboration of concept of the modernization concept for operating I&C system or implementation of new I&C system till its putting into stationary operation.

At all life cycle stages of the NPP I&C system the licensing expert review of nuclear and radiation safety is performed. The expert review consists in assessment of compliance of the NPP I&C system with requirements of guides, rules and standards on NRS on the basis of information presented in documents substantiating safety of NPP I&C system.

Expert activity is a labor-intensive process, during which experts need to analyze and assess a considerable amount of different information. A modern level of development of computer and software technologies allow performing automation of information support to expert activity (in particular, in the field of NPP I&C safety). As one of the principle directions of such automation, a knowledge base at NPP I&C systems and an automated system for support of expert activity in future are suggested for creation.

Development of such software is a promising direction in the development of review process and creates prerequisites for improvement of safety assessments for NPP I&C systems.

REFERENCES

Bashlykov, A. (1986). *Designing of decision-making systems in power engineering*. Moscow, Russia: Enrgoatomizdat.

Beliy, E. et al. (2008). Infomedia development concept in the state scientific and technical centre for nuclear and radiation safety. *Nuclear and Radiation Safety*, *2*, 59–68.

DSTU. (1999). *Information technologies: Processes of software life cycle*. Kiev, Ukraine: State Committee of Ukraine on Standardization, Metrology and Certification.

GND. (2000). *Methods of assessment of compliance of I&C systems important to NPP: Safety with nuclear and radiation safety requirements*. Kiev, Ukraine: State Nuclear Regulatory Administration of Ukraine.

Goldrin, V. et al. (2001). NPP instrumentation and control systems safety standardization and assessment (3), principles of hardware life extension. *Nuclear and Radiation Safety*, *2*, 24–29.

GOST. (1992a). *Information technology: Types of testing of automated systems*. Moscow, Russia: Publishing House of Standards.

GOST. (1992b). *Information technology: Complex of standards on automated systems: Automated systems: Stages of creation*. Moscow, Russia: Publishing House of Standards.

IAEA. (2002). *Instrumentation and control systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IEC. (2008). *Functional safety of electrical/electronic/programmable electronic safety/related systems*. IEC.

IEC. (2011). *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*. IEC.

ISO/IEC. (2008). *Systems and software engineering – Software life cycle processes*. ISO/IEC.

Kharchenko, V. et al. (2002). NPP instrumentation and control systems safety standardization and assessment (7), regulatory requirements on software. *Nuclear and Radiation Safety*, *1*, 18–33.

Kharchenko, V., et al. (2004). *Methods of modeling and assessment of software quality and dependability*. Kharkov, Ukraine: Zhukovsky National Aerospace University KhAI.

Kharchenko, V., & Sklyar, V. (2008). *FPGA-based NPP instrumentation and control systems: Development and safety assessment*. Kharkov, Ukraine: Zhukovsky National Aerospace University KhAI.

Khvastunov, R. et al. (1981). *Expert assessments and their application in power engineering*. Moscow, Russia: Energoizdat.

Klevtsov, A. (2007a). The knowledge base for safety assessment of NPP's instrumentation and control systems. *Radio Electronic and Computer Systems*, *7*, 114–120.

Klevtsov, A. (2007b). Creating and using of knowledge base for support of expert activity. *Nuclear and Radiation Safety*, *1*, 86–97.

Klevtsov, A. (2008a). Development of automated system for support of expert activity during safety assessment of instrumentation and control systems. In *Modeling and analysis of safety and risk in complex systems: Proceedings of international scientific school MASR-2008* (pp. 420–425). Saint Petersburg, Russia: Saint-Petersburg State University of Aerospace Instrumentation.

Klevtsov, A. (2008b). The model for safety assessment of NPP's instrumentation and control systems under nuclear and radiation safety expert reviewing. *Radio Electronic and Computer Systems*, *7*, 53–58.

Klevtsov, A., & Yastrebenetsky, M. (2007c). Perspectives of developing and using of knowledge base at NPP's I&C for expert activity support. In *Proceedings of International Conference on Knowledge Management in Nuclear Facilities: Book of Extended Synopsis* (pp. 119-120). Vienna, Austria: IAEA.

Konorev, B. et al. (2007). Target technology of cost-effective assessment of reliability and functional safety of critical software. *Radio Electronic and Computer Systems*, *6*, 162–170.

Konorev, B. et al. (2010). Independent verification and prediction of hidden defects of software of critical systems: Complex of static analysis tools. In *Problems of safety assurance of NPP instrumentation and control systems: Collected articles* (pp. 152–156). Odessa, Ukraine: Astroprint.

Larichev, O. (2008). *Theory and methods of decisions-making*. Moscow, Russia: Logos.

Law of Ukraine. (1995). *On nuclear energy use and radiation safety*. Kiev, Ukraine: Verkhovna Rada of Ukraine.

Law of Ukraine. (2000). *On authorizing activity in nuclear energy use*. Kiev, Ukraine: Verkhovna Rada of Ukraine.

Lindner, A., & Wach, D. (2008). Experiences gained from independent assessment in licensing of advanced I&C systems in nuclear power plants. *Nuclear Technology*, *143*, 197–207.

Miedl, H. (2010). Qualification of field equipment with software for systems important to safety. In *Problems of safety assurance of NPP instrumentation and control systems: Collected articles* (pp. 133–166). Odessa, Ukraine: Astroprint.

NP. (2000). *Nuclear and radiation safety requirements on instrumentation and control systems important for safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Administration of Ukraine.

NP. (2005a). *Procedure for state review of nuclear and radiation safety*. Kiev, Ukraine: State Nuclear Regulatory Administration of Ukraine.

NP. (2005b). *Requirements for modification of nuclear plants and an order of their safety assessment*. Kiev, Ukraine: State Nuclear Regulatory Administration of Ukraine.

Sergienko, V. et al. (2008). Calibration of invariants measurements methods of critical software: Profile of injecting test faults. *Radio Electronic and Computer Systems*, *5*, 161–167.

Sklyar, V., & Kharchenko, V. (2006). Safety features and assessment of software of NPP instrumentation and control systems. *Nuclear Measuring-Information Technologies*, *1*, 3–18.

Tokarenko, V. (2000). System of safety analysis of atomic technologies SABAT. *Issues of Atomic Science and Technique*, *3*, 45–70.

USNRC. (2010). Standard review plan for the review of safety analysis reports for nuclear power plants: LWR Ed. section 7.0: Instrumentation and control - Overview of review process (rev. 6). Washington, DC: US Nuclear Regulatory Commission.

Yastrebenetsky, M. et al. (2001a). NPP instrumentation and control systems safety standardization and assessment (1), objects, aims, tasks. *Nuclear and Radiation Safety*, *1*, 20–28.

Yastrebenetsky, M. et al. (2001b). NPP instrumentation and control systems safety standardization and assessment (2), principles of standardization. *Nuclear and Radiation Safety*, *2*, 16–23.

Yastrebenetsky, M. et al. (2001c). NPP instrumentation and control systems safety standardization and assessment (4), principles of assessment. *Nuclear and Radiation Safety*, *3*, 17–30.

Yastrebenetsky, M. et al. (2001d). NPP instrumentation and control systems safety standardization and assessment (5), regulatory requirements on systems. *Nuclear and Radiation Safety*, *3*, 31–37.

Yastrebenetsky, M. et al. (2001e). NPP instrumentation and control systems safety standardization and assessment (6), regulatory requirements on hardware. *Nuclear and Radiation Safety*, *4*, 11–25.

Yastrebenetsky, M. et al. (2002a). NPP instrumentation and control systems safety standardization and assessment (8), automatic control algorithms assessment. *Nuclear and Radiation Safety*, *2*, 23–36.

Yastrebenetsky, M. et al. (2002b). NPP instrumentation and control systems safety standardization and assessment (9), procedures of assessment and their information support. *Nuclear and Radiation Safety*, *3*, 40–57.

Yastrebenetsky, M. et al. (2004). *Safety of nuclear power plants: Instrumentation and control systems*. Kiev, Ukraine: Technique.

Yastrebenetsky, M., et al. (2012). Strategy of NPP I&C systems modernization in Ukraine. In *Proceeding of 8th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 593-599). San Diego, CA: American Nuclear Society.

Yastrebenetsky, M., & Vasilchenko, V. (2001f). Expert evaluation in NPP safety important systems licensing process. In *Proceedings of the 9-th International Conference on Nuclear Engineering*. Nice, France: Academic Press.

KEY TERMS AND DEFINITIONS

Expert Review of Nuclear and Radiation Safety: Assessment of documents, substantiating safety of NPP I&C systems, for compliance with NPP safety principles and also the main requirements of nuclear and radiation safety assurance, determined in legislative and regulatory documents in force.

Knowledge Base: Computer system devoted to acquisition, storage and representation of knowledge in a specific subject area.

Licensing: Authorization for performing activities connected with use of NPP and sources of ionizing radiation.

Life Cycle: A set of stages in creation, implementation and use of a system (system component) within a time period that starts from the moment of concept development and determination of technical requirements and ends in the moment of removal of system (system component) from operation due to impossibility or inexpediency of further intended use.

NPP I&C Safety: A part of nuclear and radiation safety, relating to jointly operating I&C systems and manufacturing equipment of NPP power units and depending on proper operation of the I&C systems.

NPP Nuclear and Radiation Safety: A feature of non-exceeding determined limits of radiation effects on personnel, the population and the environment under NPP normal operation, operational events and design basis accidents and also of restricting radiation effects in beyond design basis accidents.

Safety Regulation: Regulation of safety principles in order to ensure safety of people, environment, nuclear facilities and sources of ionizing radiation.

APPENDIX: ADDITIONAL READING

IAEA Scientific and Technical Publications

IAEA (2000). NS-G-1.1. *Software for computer-based systems important to safety in nuclear power plants. Safety guide*. Vienna, Austria: IAEA.

IAEA. (1998). TECDOC-1016. *Modernization of Instrumentation and Control in nuclear power Plants*. Vienna, Austria: IAEA.

IAEA. (1999). *Modern Instrumentation and Control for Nuclear Power Plants. A Guidebook*. Vienna, Austria: IAEA.

The Main IEC Standards

IEC (2004). IEC 62138. *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*.

IEC (2006). IEC 60880. *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*. Ed. 2.

IEC (2007). IEC 62340. *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*.

Other Scientific and Technical Publications

Andrashov, A., et al. (2007). The static analysis of a program code procedure based on metrics profiling. *Radio electronic and computer systems, 8*, 184-188. (in Russian).

Courtois, P.-J. (2001). Software important to safety: the new IAEA Safety Guide and the common position of European nuclear regulators. *Proceedings of CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-based I&C Systems* (pp. 117-128). Hluboka nad Vltavou, Czech Republic.

Courtois, P.-J. (2008). *Justifying the Dependability of Computer-based Systems*. Springer.

Eagle, E.O. (2012). Lessons learned from instrumentation and controls licensing reviews of combined license applications that use earlier certified designs. *Proceeding of 8th International topical meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 1283-1290). San Diego, USA: American Nuclear Society.

GOST 27.310. (1995). *Dependability in technics. Failure Mode, Effect and Criticality Analysis. Basic principles*. Moscow, Russia: Publishing House of Standards. (in Russian).

Jung, I. (2012). Regulatory perspectives and lesson learned from USNRC new reactor instrumentation and control licensing review. *Proceeding of 8th International topical meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 733-742). San Diego, USA: American Nuclear Society.

Klevtsov, A. (2008). The experience of nuclear and radiation safety expert reviewing of new and modernized NPP'S instrumentation and control systems. *Radio electronic and computer systems, 6*(33), 122-127. (in Russian).

Klevtsov, A., et al. (2010). Principles of developing the knowledge portal on safety of nuclear facilities. *Nuclear and Radiation Safety, 3*, 53-57. (in Russian).

Ponomarenko, T., Klevtsov, A. (2002). On use of software analysis tools for software assessment and analysis of NPP. I&C systems. *Nuclear and Radiation Safety, 4*, 71-80 (in Russian).

Sklyar, V., et al. (2006). Assessment of software of NPP. control system with the use of instrumental tool LDRA Testbed. *Nuclear and Radiation Safety, 2*, 83-98. (in Russian).

Sklyar, V., et al. (2008). An assessment of software of nuclear power plants instrumentation and control systems in expertise of nuclear and radiation safety. *Radio electronic and computer systems, 6*, 180-185. (in Russian).

Sklyar, V., et al. (2012). Comparing of licensing approaches for FPGA-based safety I&C platforms. *Proceeding of 8th International topical meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 1558-1568). San Diego, USA: American Nuclear Society.

Sklyar, V., & Beliy, Yu. (2006). Metrical assessment of software changes of instrumentation and control systems. *Radio electronic and computer systems, 6*, 147-152. (in Russian).

Stamatis, D.H. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution*. USA: ASQ Quality Press.

Stiffler, C.D., & Odess-Gillett, W. (2012). Experiences and lessons learned on licensing instrumentation and control systems in the United Kingdom. *Proceeding of 8th International topical meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 1219-1227). San Diego, USA: American Nuclear Society.

USNRC (2011). DI&C-ISG-06. Digital Instrumentation and Controls. Licensing process. Interim staff guidance.

Wiegand, C. (2012). Challenges and lessons learned in I&C design and licensing for FOUR new nuclear plants in China. *Proceeding of 8th International topical meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 197-199). San Diego, USA: American Nuclear Society.

Yastrebenetsky, M., et al. (2005). Indices of functional safety of NPP. init control system. *Nuclear measuring-information technologies, 3*, 67-74.

Yastrebenetsky, M., et al. (2006). Evaluations of NPP. I&C Functional Safety Measures. *Proceeding of 5th International topical meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 1-7). Albuquerque, USA: American Nuclear Society.

Chapter 13
NPP:
Power Grid Mutual Safety Assessment

Eugene Brezhnev
Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Vyacheslav Kharchenko
National Aerospace University named after N.E. Zhukovsky KhAI,
& Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

ABSTRACT

The problem of the safe interaction between a Nuclear Power Plant (NPP) and a Power Grid (PG), considering the Fukushima nuclear accident, is becoming topical. There are a lot different types of influences between NPPs and PG, which stipulate NPPs' safety levels. To evaluate the influences, two metrics are proposed: linguistic and numerical. The approach to the NPP-PG safety assessment is based on the application of Bayesian Belief Network (BBN), where nodes represent different PG systems and links are stipulated by different types of influences (physical, informational, geographic, etc). It is suggested to evaluate criticality of the PG system considering the change of criticalities of all connected systems. The total criticality of each node in BBN is assessed considering particular criticalities caused by different types of influence. The complex nature of NPP and PG mutual interaction calls for the need for integration of different methods that use input data of different qualimetric nature (deterministic, stochastic, linguistic). Application of one specified group of risk methods might lead to loss and/or disregard of a part of safety-related information. BBN and Fuzzy Logic (FL) represent a basis for development of the hybrid approach to capture all information required for safety assessment of NPP – PG under uncertainties. Integration of FL-based methods and BBNs allows decreasing the amount of input information (measurements) required for safety assessment, when these methods are used independently outside from the proposed integration framework. An illustrative example for the NPP reactor safety assessment is considered in this chapter.

INTRODUCTION

The reliable and safe operation of the energy sector is of key importance for the any national economic development, as both production and municipal facilities require electric power for their operation. The power industry consists of power

DOI: 10.4018/978-1-4666-5133-3.ch013

generating system, high voltage transmission system, lower voltage distribution system and other support facilities.

Three types of generation facilities are operated in Ukraine, including thermal power plants (steam turbine and diesel types), hydroelectric plants (hydroelectric proper and hydroelectric accumulating plants) and NPPs. Thermal power plants account for about 50% of the electric power produced in Ukraine. Most of these thermal power plants (TPPs) are old, with antiquated equipment, obsolete technology, and largely lacking modern pollution control equipment. Only about 10% of Ukraine's TPPs had undergone any significant reconstruction.

The major fuel for the plants is natural gas (76-80%), but they also use black oil (15-18%), and coal (5-6%). Most steam power plants have outdated equipment, which does not correspond to present-day environmental requirements, and calls out for reconstruction, upgrade, or complete replacement.

Ukraine's four nuclear power stations operate 15 reactors with a capacity of 13,8 Giga watts (GW), or nearly one-quarter of the country's total. They generate around 88,8 GW of energy, or over 47.9% of the country's power output, with the construction of two reactors with a capacity totaling 2 gigawatts (GW) in its final stages. Power reactors have operated in Ukraine since 1977, and over 300 reactor years of operating experience have been accumulated.

Power resources of Ukraine are mainly formed by domestic generation capacities (nearly 98%), with the import share being insignificant (2%). The power is largely consumed inside the country (97%), with a small part exported (3%). In the future, the need for power is expected to grow calling for intensification of the sector development and optimizing of the organization structure and economic mechanisms of functioning in the market environment.

Ukraine's electric networks are numbered nearly 22, 7 thousand km., 4,9 thousand km. of them are under voltage 400-750 kW (high voltage transmission lines), 13,2 thousand km. – under 330 kW, 4,6 thousand km. 220-110 kW (lower distribution lines). Their conditions are getting more aggravated every year. 34% of overhead transmission lines (220-330 kW) have been operating nearly 40 years. Approximately 52% of them have to be renovated, 76% of transformer substations have reached the end of their service life.

BACKGROUND

All facts mentioned above are given to show the high complexity of Ukrainian energy sector and problem of its reliability assurance. Reliable operation of the NPP implies that PG, to which it is connected, is reliable. Disturbances in PG operation can originate from natural disasters, failures, human factors, terrorism, and so on.

If PG and NPP are considered together as SoS, we can conclude that PG reliability and safety are stipulated by the NPP safety. Outages and faults will cause serious problems and failures in the interconnected power systems. It means that unsafe power grid and NPP could be considered mutual risk factors undermining the safety of both facilities. In order to provide stable and safe operation of NPPs, a systematic way of formalization and evaluating these influences is needed.

The object of the chapter – is to introduce approaches and techniques, which allow to evaluate the mutual influences between NPP and PG, understand the dynamic risks nature caused by their interactions.

The techniques represented in the chapter can be considered an essential part of PG risk management and can serve as a base for decision-making to avoid disturbances or minimize the severity of their consequences considering the interaction between NPP and PG systems. These techniques allow understanding the risk proliferation and develop the recommendations and measures for NPP safety assurance.

NPP – POWER GRID SAFETY ASSESSMENT BASED ON MUTUAL INFLUENCE ANALYSIS

Approach for NPP-PG Influence Formalization

Key technical problems of power industry of Ukraine, which could lead to NPPs' disturbances (Tsarenko et al., 2008, differgroup.com) are:

1. The production capacities in Ukrainian electricity sector are outdated: nearly 95% of power units have worked out their useful life, the residual life of thermal power plants is 5-7 years. Currently 95% of power units already worked out their normal service life (100 000 hours), more than a half have been working for 200 000 hours. 80% of power plants have been operating for 30 years. Such a deterioration was stipulated by low quality fuel, fickle regime of TPPs capacities due to poor maneuverability and lack of funds for reconstruction. NPPs will approach the end of their designed service life in 2011-2030. This poses a problem for the possible equipments' failures.
2. There is a lack of maneuverability capacities in Ukraine, a share of electricity produced by Hydro power station (HPS) accounts for about 10,2%.
3. The level of technological losses constitutes 14.4% of the electricity produced, which is 2-2.5 higher than in developed countries. It is necessary to modernize the transmission and distribution networks. The growing demand for electricity cannot be satisfied using the old transmission and distribution networks.

All technical problems mentioned could stipulate the risks associated with the NPP-PG interaction. There are some extra causes beside all mentioned, which could lead to the disturbances of power grid. They are classified as internal and external basic causes.

The basic internal causes, which lead to disturbances of the power grid's operational mode (NUREG-75/014, 1998), are:

- The stable short circuit on the high–voltage transmission lines followed by their removal from service (50-70% out of - all power grid accidents) (it caused the blackout 2003);
- The short circuits, which stipulate the activation of differential bus protection (more than 10%);
- The emergency shutdown of the power block (near 5%);
- The staff's errors (near 5%).

The basic external causes, which lead to disturbances of the power grid's operational mode:

- The seismic vibration;
- The wind influences on power grid's facilities;
- The icing on transmission lines (quite frequently in Ukraine);
- The natural disasters (fires, flooding, hurricanes, pollutions).

Grid interconnectivity and redundancies in transmission paths and generating sources are key elements in maintaining reliability and stability in high performance grids. However, operational disturbances can still occur even in well maintained grids. Similarly, even an NPP running in base load steady-state conditions can encounter unexpected operating conditions that may cause transients or a complete shutdown in the plant's electrical generation. When relatively large NPPs are connected to the electric grid, abnormalities occurring in either can lead to the shutdown or collapse of the other.

The NPPs and electric transmission grids are complex engineering facilities, which determine the persistent economic development of any countries. When they are connected together in a controlled, dynamic and distributed network, further complexity is created. This complexity of engineered systems is a consequence of several factors: the sheer size and interconnectivity of the electric grid, the nuclear safety requirements imposed on NPPs the need to balance electricity supply and consumption throughout the grid at all times, and die nature of electricity – that it is generated as it is used. Unlike other commodities, it is difficult to store electricity. This means the electric grid system requires continual surveillance and adjustment to ensure supply always matches demand. Unlike NPPs, the inherent, natural and passive safety feedback systems based on physical laws are rather weak. Hence electric grids require continuous control and balancing actions based on engineered systems.

Stability in the grid system is maintained by matching the electricity generation with the ever changing demand. The electricity from many power generating stations is "pooled" in the transmission system, and each customer draws from this pool. Power, entering the system, flows along all available paths to the distribution systems. This pooling of electricity also means that power is provided from a variety of generating stations of different sizes, including nuclear, coal, oil, natural gas and renewable energy sources such as wind, solar, biomass and hydro power, which must all he synchronized to the same rhythm with millisecond accuracy. For a power grid to remain stable, the frequency and phase of all power generation units must remain synchronous within narrow limits. A generator that loses synchronism with other generators but stays connected to the grid will experience large electrical currents, which will lead to overheating and large mechanical forces that will rapidly destroy the generator. So protective circuit breakers disconnect (trip) a generator from the grid, when the generator loses synchronism.

The reliability of off-site power is usually assured by two or more physically independent transmission circuits to the NPP to minimize the likelihood of their simultaneous failure. Similarly, the reliability of on-site power is enhanced by sufficient independence, redundancy and testability of batteries, diesel generators, gas turbines and the on-site electric distribution systems to perform safety' and other functions even if a single failure occurs. Because of the importance of reliable off-site power as well as considerations of cost effectiveness and efficiency, the electric grid is an important factor in NPP site selection, which must take into account the plant's position within the grid as well as its proximity to centres of electricity demand, population density and other factors.

In addition to assuring that the electric grid will provide reliable off-site power to NPPs, there are other important factors to consider, when an NPP will be the first nuclear unit on the grid and, most likely, the largest unit. If an NPP is too large for a given grid, the operators of the NPP and the grid may face several problems.

Off-peak electricity demand might be too low for a large NPP to be operated in base load mode, i.e. at constant full power.

There must be enough reserve generating capacity in the grid to ensure grid stability during the NPP's planned outages for refueling and maintenance.

Any unexpected sudden disconnect of the NPP from an otherwise stable electric grid could trigger a severe imbalance between power generation and consumption causing a sudden reduction in grid life.

The technical issues associated with the interface between NPPs and the electric grid includes (NUREG-1150, 1989):

- The magnitude and frequency of load rejections and the loss of load to NPPs;

- Grid transients causing degraded voltage and frequency in the power supply of key safety and operational systems of NPPs;
- A complete loss of off-site power to an NPP due to grid disturbances;
- An NPP unit trip causing a grid disturbance resulting in severe degradation of the grid voltage and frequency, or even to the collapse of the power grid.

Influence of Grid Disturbances on Nuclear Power Plants

Load Rejection and Complete Loss of Load. A load rejection is a sudden reduction in the electric power demanded by the grid. Such a reduction might be caused by the sudden opening of an interconnection with another part of the grid that has carried a large load. An NPP is designed to withstand load rejections up to a certain limit without tripping the reactor. An NPP's ability to cope with a load rejection depends on how fast the reactor power can be reduced without tripping and then how fast the reactor power output can be increased hack to the original level, when the fault is cleared. Load rejections of up to 50% are accommodated by a combination of several actions: rapidly running back the steam turbine to the new lower demand level, diverting the excess steam from the turbine to the main steam condenser unit or to the atmosphere if this is permitted by licensing regulations, and reducing reactor power via insertion of control rods without tripping the reactor.

A *loss of load* is a 100% load rejection that is the entire external load connected to the power station is suddenly lost, or the breaker at the station's generator output is opened. Under this severe condition, it may still be possible to 'island' the NPP so that it powers only its own auxiliary systems. During this 'house-load' operating mode, the reactor operates at a reduced power level that is still sufficient to assure enough electricity for its own needs, typically 5% of full power. Once the grid disturbance has been eliminated, the NPP can be re-synchronized to the grid and its production quickly raised again to full power. This operational characteristic of the NPP is important, when the loss of load is expected to last for just a short time.

Degraded Grid Voltage or Frequency. Electric grids are controlled to assure that a particular frequency, either 50 or 60 Hz, is maintained within a small tolerance, typically within ± 1%. When the grid develops an imbalance between generation and load, the grid frequency tends to 'droop' if the *load exceeds generation and increase if generation exceeds the load.* A reduction in frequency can be caused by several events, such as insufficient available generation, a major electrical disturbance, such as a circuit fault or the trip of a major generator unit. A small droop in the grid frequency caused by the loss of generation can be controlled by quickly activating the grid's available "spinning reserve," either automatically or manually, starting up additional generation capacity, such as gas turbines or hydroelectric power, and disconnecting selected loads (i.e. customers) from the grid (load shedding).

Isolating the section of the grid with the NPP from the rest of the grid ('system islanding') can also help maintain the proper frequency in the islanded system. System islanding may reduce the load on the NPP, requiring that its generation be reduced accordingly by a quick set-back to an intermediate power level. Proper islanding prevents the NPP from tripping because of the lower frequency, but may further aggravate the power imbalance in the rest of the grid. A plant trip including reactor shutdown should be regarded as a last resort. During a trip the plant is subject to rapid changes in power, pressure and temperature, which shorten the lifetime of the plant. Moreover, if the NPP is immediately disconnected from the grid, the lost generation will exacerbate the degraded conditions on the grid.

Any change in the grid frequency affects an NPP's operation by changing the speed of the NPP's turbo generator and the speed of pumps circulating coolants through the reactor and die secondary coolant circuits. The main reactor circulating pumps, steam generator feed water pumps and long term decay heat removal systems rely on stable electric power to function properly. The speed of the reactor's main coolant pumps is directly proportional to the frequency of the electric power supply. Therefore, if the frequency of the power from the grid drops far enough, the pumps will slow, which will lead to inadequate core cooling, and the reactor w ill trip.

Other AC motors in the NPP may also trip due to rising currents and consequent overheating caused by reduced frequency. The performance of AC motors is directly affected by the voltage and frequency of their power supplies. If electric grid voltages are not sufficient, motors cannot develop sufficient motor torque to start, and if the frequency drops below a certain value, the start and operation of AC motors would require higher operating voltages. If the voltage is insufficient, it results in excessive current being drawn by the motor that in return would lead to overheating and the opening of protective breakers.

The frequency and voltage ranges, in which large AC motors can operate, are relatively narrow. Thus, in severely abnormal conditions, safety systems in nuclear power plants are required to take protective actions such as tripping the reactor and turbine, separating the plant electrical systems from the degraded conditions present on the grid, and switching to on-site emergency power sources until the grid voltage and frequency are restored to acceptable values. These actions protect the NPP by safely shutting it down and keeping it cooled. However, any sudden automatic shutdown of a large baseload nuclear unit during periods, where there is already a mismatch between generation and load on the grid can only further degrade the grid's condition, potentially leading to a partial or full collapse.

Loss of Off-Site Power. Any loss of off-site power would he caused by external events beyond the NPP's switchyard, such as transmission line faults and weather effects like lightning strikes, ice storms and hurricanes. A loss of off-site power interrupts power to all in-plant loads, such as pumps and motors, and to the NPP's safety systems. As a protective action, safety systems will trigger multiple commands for reactor protective trips (e.g. turbine and generator trip, low coolant flow trip, and loss of feedwater flow trip). The reactor protection system will also attempt to switch to an alternate off-site power source to remove residual heat from the reactor core. If this fails, in-plant electrical loads must be temporarily powered by batteries and stand-by diesel generators until off-site power is restored. However, diesel generators may not be as reliable as off-site power from the grid in normal conditions. Diesel generators may fail to start or run 1% of the time. However, the probability of failure can be significantly reduced by installing independent trains of diesel generators. Batteries can provide power only for a limited time.

Influence of NPP Disturbances on the Grid

Trip of an NPP Causing Degraded Grid Frequency and Voltage. Even at steady state conditions, when the generation and loads on a grid are in balance, if a large NPP (e.g. 10% of the grid's total generating capacity) trips unexpectedly, the result can be a significant mismatch between generation and load on the grid. Unless additional power sources are quickly connected to the grid, this can degrade the grid's voltage and frequency and, thus the off-site power supply to the NPP. The degraded voltage and frequency on the grid can potentially result in the NPP protection system disconnecting the degraded off-site power to the NPP. This will force the NPP to switch to on-site emergency power to run safety and core cooling systems until off-site power is restored. This should be done as soon as possible for safety reasons: the possible concurrent failure of the NPP's on-site power system and delayed recovery of off site electric power would make it nearly impossible in most NPPs to cool the core, a situation that must he avoided under all conditions. The introduction of new reactor designs that use passive cooling would alleviate this problem. Therefore in unreliable grid systems it is recommended to consider NPP designs with passive safety systems.

The grid's response over time to the sudden loss of the NPP can be modeled by computer simulations, conditioned by the capacity and interconnectivity of the grid and the size of the lost NPP generation, as well as the timing of switching additional power sources to the grid. Large interconnected electric grids can usually meet the requirement of providing reliable off-site power to NPPs connected to the grid. However, in some scenarios involving poorly interconnected or controlled electric grids, the sudden shutdown of a large NPP or any other large generating station elsewhere on the grid, might result in severe degradation of the grid's voltage and frequency, or even to the collapse of the overall power grid. Similarly, when an NPP is sited on a well maintained but small and isolated grid of limited generating capacity (e.g. on an island), the sudden loss of its generation may lead to the same outcome.

Types of Influences

The NPP as a part of PG constantly interacts with other elements of PG. All influences (or relationships) existed in PG could be divided into several hierarchy's levels.

The first level of a hierarchy is a level of interaction between NPPs and TPPs, HPs as other generating systems. They could interact indirectly by means of transmission and distribution networks. On this hierarchy's level systems influence each other as a whole.

Generally influences could be classified into different types (Dudenhoeffer, 2006):

1. Physical $I_{phys}^{NPP}(t)$: A physical reliance on materials flow from one infrastructure to another. This physical reliance could be of two types: internal and external. The internal reliance refers to electrical flow between NPP and other PG's elements. The external reliance refers to PG's interactions with other infrastructures. For example a thermal power plant generating 1,000 mW typically consumes 10 000 tons of coal per day. Under normal operating conditions the PG requires natural gas and petroleum fuels for its generators, road and rail transport and pipelines to supply fuels to generators, water for cooling and emissions control, banking and finance for fuel purchases etc.
2. Informational $I_{\inf}^{NPP}(t)$: A reliance on information transfer between NPP and other elements of PG (via through I&C systems). NPP-PG state depends on information transmitted through the information infrastructure. Informational dependencies connect NPP and other PG elements via electronic, informational links.
3. Geographic $I_{geo}^{NPP}(t)$: A local environmental event affects components of NPP-PG (usually the transmission lines) due to physical proximity. Given this influence, events such as an explosion or fire could create correlated disturbances or changes in these NPP-PG elements.
4. Logical $I_{\log}^{NPP}(t)$: An influence that exists between NPP - PG that does not fall into one of the about categories. Logical dependencies may be more closely likened to a control scheme that links PG's elements without any direct physical, informational, geographical connections (all indirect influences, example – Moscow blackout 2005 resulted to banking systems disturbances).
5. Organizational $I_{org}^{NPP}(t)$: Influences though policy, regulation, markets. The influence that exists due to a policy or procedure that relates a state change in one elements of PG

to subsequent effect on another components;

6. Societal influence $I_{soc}^{NPP}(t)$ that PG components may have on societal factors as public opinion, fear and confidence.

Mutual PG-NPP safety influence is shown on Figure 1. It is worth to note that influence exists on all grid levels and has to be taken into consideration when providing grid systems safety.

There are some influence types on lower levels of NPP-PG's hierarchy.

All influences of subsystem's level might be divided in following categories:

- **Functional Influence:** Connected equipment encompasses NPP and other PG's elements design involving shred equipment, common input, loop dependencies plus situations, in which the same equipment provides multiple functions. Nonconnected equipment encompasses interrelated success criteria such as the relationships between standby system and the system it is supporting;
- Cyber influences via control systems;
- **Spatial Influences:** Refers to equipment within small distance to each other;
- **Human Influences:** Refers to all activities with human participation.

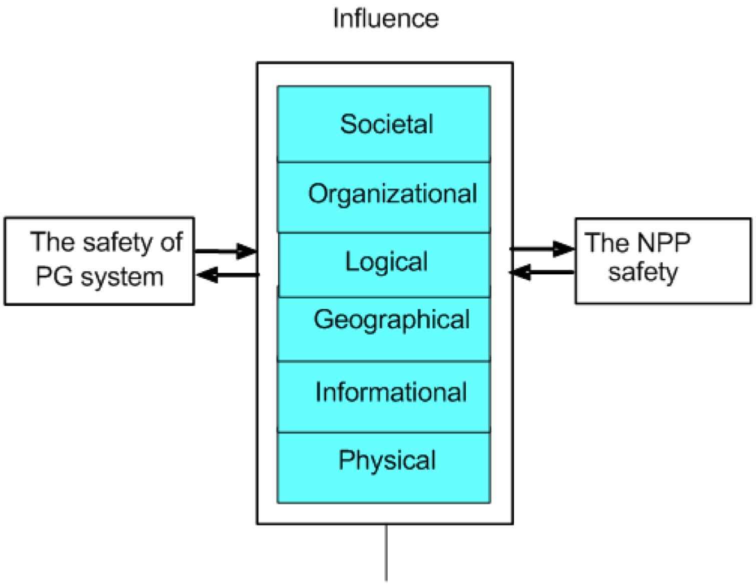
Influences Formalization

As we see, there are a lot of different types of influences, which exist on all NPP-PG hierarchy's levels. Though these influences create opportunities, they also create new vulnerabilities. These vulnerabilities may produce adverse impacts that are becoming more widespread and more frequent.

In order to provide stable and safe operation of NPPs, a systematic way of formalization and evaluating these influences are needed.

The influences between different systems of PG could be described (or formalized) by means of the Influence vector (Brezhnev et al., 2011). The *Influence vector* is characterized by the value and direction. The direction points the initial source

Figure 1. Mutual PG-NPP safety influence



of influence and systems being under influence. The value characterizes the strength of influence.

The influences between NPP and PG elements could be represented by a matrix of influence shown in the Table 1.

The influence matrix shows how elements of the system influence each other and strength of their influence. As an example, NPP influences TPP with a strength – medium and HPP with high level of influence. Generally, influence is an ability of one system to determine the state, characteristics and behavior of other systems.

To evaluate the influences between NPP and power grid systems we need to have the metrics by which this influences could be measured and compared. Two types of metrics: linguistic and numerical are suggested. The linguistic metric operates with the linguistic values used to evaluate the strength of influence. The different values as high, medium and low are applied to consider and predict the smart grid's system state changing provided the accident in other SG system occurred. Numerical values, as ranks, are used in the similar way, and the different ranks stand for the different strength of influence. Expert judgments are considered as the basis for taking the influence values. The influence database is completed for each NPP. These values are regularly updated.

Space of Influence

NPP could influence the power grid in the different ways as physically, geographically, organizationally, by means of information, logically, societal, etc. Thus, we introduce the space of influence. Physical, geographical, organizational, informational, logical, societal is a particular influence.

Table 1. Matrix of influence

	NPP	TPP	HPP
NPP	-	M	H
TPP	L	-	
HPP	M		-

Total influence might be represented as:

$$I_t^{NPP}(I_{geo}^{NPP}(t), I_{phys}^{NPP}(t), I_{org}^{NPP}(t), I_{soc}^{NPP}(t), I_{\log}^{NPP}(t)) \quad (1)$$

The total influence is a time dependable value. The changes of NPP states and characteristics stipulate the changes of the total influence value.

We could illustrate the particular influence, for example geographical influence of NPP on other system of power grid shown in Figure 2.

Formally, the geographical influence of NPP on other systems of power grid might be written as:

$$\bar{I}_{geo}^{NPP}(t) = \left\{\bar{I}(NPP \to TPP), \bar{I}(NPP \to HPP), \bar{I}(NPP \to TG)\right\} = = \{Medium(M), High(H), Low(L)\}. \quad (2)$$

The value of geographical influence could be calculated as:

$$I_{geo}^{NPP} = \sum_{i=1}^{I} I_{geo}^{i}(NPP \to SPG_i) = \mathrm{H} + \mathrm{M} + \mathrm{L}. \quad (3)$$

Figure 2. Geographical influence

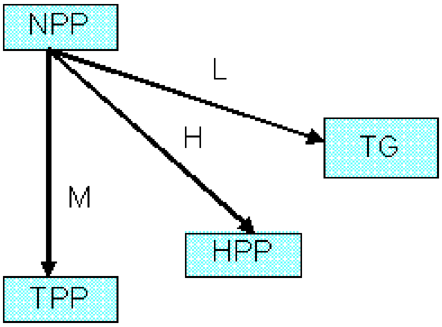
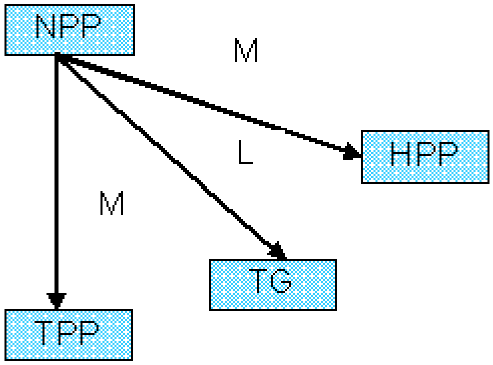


Figure 3. Organizational influence



Similarly, the organizational influence might be represented as shown in Figure 3.

The value of organizational influence could be calculated as:

$$I_{org}^{NPP} = \sum_{i=1}^{I} I_{org}^{i}(NPP \to SPG_i);$$

$$I_{org}^{NPP} = \sum_{i=1}^{I} I_{org}^{i}(NPP \to SPG_i)\text{=M + L + M.} \tag{4}$$

The total influence value might be calculated as a sum of the particular influence values on all influence space existed for NPP-PG system.

The total influence value calculated as a sum of the particular influence values characterizes the absolute influence of NPP on other PG systems. For each systems of power grid could be evaluated their total influences. Their ranking might determine the most and least influential system. In Table 2 the different influences' factors are combined.

It helps to estimate the value of total influence, for instance, NPP on all of subsystems as:

$$\begin{gathered}
I_{tot}^{NPP}(I_{phys}^{NPP}(t), I_{geo}^{NPP}(t), I_{org}^{NPP}(t), I_{\inf}^{NPP}(t),..., I_{soc}^{NPP}(t)) - \\
total\ NPP's\ \inf luence; \\
I_{phys}^{NPP}(t) = \sum_{i=1}^{I} I_{phys}^{i}(NPP \to SPG_i); \\
I_{geo}^{NPP}(t) = \sum_{i=1}^{I} I_{geo}^{i}(NPP \to SPG_i),...; \\
I_{tot}^{NPP} = w_{phys}(H + M + L) + \\
w_{geo}(M + L + H) + w_{org}(M + H + L) + ..., \\
SPG_i - S_i\ of\ power\ grid.
\end{gathered} \tag{5}$$

We shall consider the relative influence value $I_{rel}(t)$. The relative influence value determines the influence of one system on another system, for example NPP on TPP. It might be calculated as:

$$\begin{gathered}
I_{rel}(NPP \to TPP) = I_{geo}(NPP \to TPP) + \\
I_{org}(NPP \to TPP) + \\
... + I_{soc}(NPP \to TPP).
\end{gathered} \tag{6}$$

The different types of NPP's relative influence are shown in Figure 4.

Similarly, the relative influences of different power grid systems might be evaluated for NPP.

Table 2. The combined matrix of influences

	Physical				Geographical				Informational			
	NPP	**TPP**	**HPP**	**DG**	**NPP**	**TPP**	**HPP**	**DG**	**NPP**	**TPP**	**HPP**	**DG**
NPP	0	M	L	H	0	H	M	L	0	M	H	M
TPP	M	0	M	L	H	0	M	L	H	0	H	H
HPP	L	H	0	H	H	L	0	H	H	L	0	H
DG	L	L	H	0	L	M	M	0	L	M	H	0

Figure 4. Relative influences of NPP

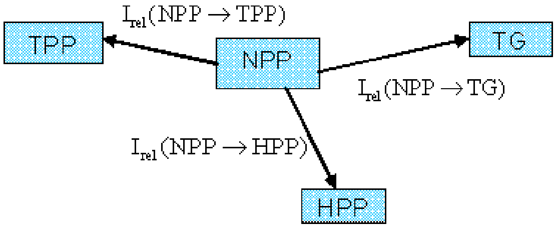
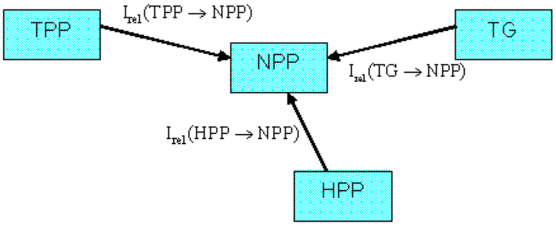


Figure 5. Relative influences on NPP



The different influences on NPP are shown in Figure 5.

It is worth to note that:

$$I_{tot}^{NPP} = \sum_{i}^{I} I_{rel}(NPP \to SPG_i). \qquad (7)$$

It might be suggested that stability of the NPP-PG system is provided by the balance of influences between its elements. The principle of infrastructure balance could be taken as one of major principle infrastructure safety assurance. The state dynamic is conditioned by changing of the balance of influences insight the system. The balance violation leads to state changing of infrastructure subsystems. According to principle of hierarchy, any system is a part of other system. One system S_1 influences another system S_2 with $I_{rel}(S_1 \to S_2)$. In the case when this value exceeds the certain value $I_{rel}^{\lim}(S_1 \to S_2)$, it might lead to state changing of S_2. The Fukushima nuclear accident proves this assumption. The NPP might stand the defined value of nature's influence. The earthquake that hit Japan was several times more powerful than the worst earthquake the nuclear power plant was built for (the Richter scale works logarithmically; for example the difference between an 8.2 and the 8.9 that happened is 5 times). In the Fukushima nuclear accident the anticipated value of influence was exceeded what resulted to accident. Let consider the NPP-Power grid system shown in Figure 6.

The infrastructure given above could be characterized by some values shown in Table 3.

In this case the conditions of safety for NPP - Power grid system given above based on the balance of influence might be written as:

$$I_{rel}(TPP \to NPP) \le I_{rel}^{\lim}(TPP \to NPP); \quad ;$$

$$I_{rel}(TPP \to T\,\&\,D) \le I_{rel}^{\lim}(TPP \to T\,\&\,D);$$

$$I_{rel}(NPP \to T\,\&\,D) \le I_{rel}^{\lim}(NPP \to T\,\&\,D);$$

$$I_{rel}(NPP \to TPP) \le I_{rel}^{\lim}(NPP \to TPP). \quad (8)$$

When the current value of influence between infrastructures exceeds the acceptable value, it could result to the state changing of one of them. The Fukushima nuclear accident proved this principle of the balance influence. The nature

Figure 6. NPP-Power grid system (general)

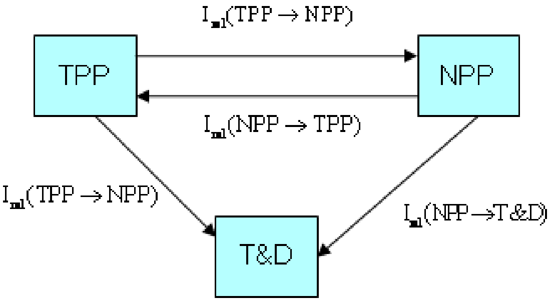


Table 3. The characteristics of influences

Relation	Current Influence	Influence limit
$TPP \to NPP$	$I_{rel}(TPP \to NPP)$	$I_{rel}^{\lim}(TPP \to NPP)$
$TPP \to T\ \&\ D$	$I_{rel}(TPP \to T\ \&\ D)$	$I_{rel}^{\lim}(TPP \to T\ \&\ D)$
$NPP \to T\ \&\ D$	$I_{rel}(NPP \to T\ \&\ D)$	$I_{rel}^{\lim}(NPP \to T\ \&\ D)$
$NPP \to TPP$	$I_{rel}(NPP \to TPP)$	$I_{rel}^{\lim}(NPP \to TPP)$

should be considered as a subsystem that influences other infrastructures. Other example of a result of the balance violation consequences is the Sayano-Shushenskaya HPP accident, when it could not withstand the increasing of load passed from Bratskaya HPP.

FMECA might be very helpful technique for formalization of influences to help performing NPP safety analysis. The traditional FMECA is the most widely used reliability analysis technique in the initial stages of system development. It is performed to assure that all potential failure modes have been considered. Traditionally, the criticality assessment is performed by calculating the failures criticality as a product of failure severity and frequency:

$$Crt(S_i) = Fr(S_i) \times Sev(S_i)\,, \qquad (9)$$

where S_i – NPP (power grid) accident, $Fr(S_i)$ – accident frequency; $Sev(S_i)$ – severity of accident's consequences.

The traditional FMECA is two dimensional. In the case when $Crt(S_1)$=$Crt(S_2)$ we need to use additional information to differ possible accidents. Therefore, the total influence $I_{tot}^{S_i}$ characterized by direction and strength might be used as third value to prioritize the possible accident. The criticality is assessed as

$$Crt(S_i) = Fr(S_i) \times Sev(S_i) \times I_{tot}^{S_i}\,. \qquad (10)$$

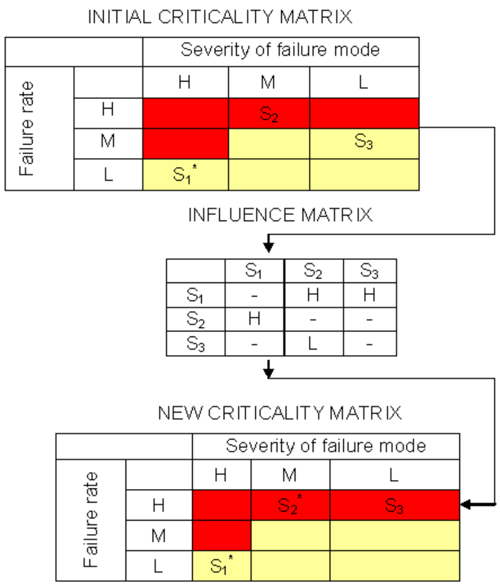
Taking into consideration the mutual influences between NPP and power grid, we assume the failure criticality of NPP (power grid) might be changed as a result of the criticality changing of power grid (NPP). We introduce the conditional criticality presented as

$$I\ (S_i^* \to S_j) : Crt(S_i \left| S_j^* \right.) = Fr(S_i \left| S_j^* \right.) \times Sev(S_i \left| S_j^* \right.) \qquad (11)$$

where $Crt(S_i \left| S_j^* \right.)$ - conditional criticality of S_i provided the failure of S_j*; $Fr(S_i \left| S_j^* \right.)$ - S_i frequency changing provided the failure of S_j*; $Sev(S_i \left| S_j^* \right.)$ S_i severity changing provided the failure of S_j*.

Any accident or a failure of the power grid system leads to the change of criticality of all related systems. When a failure of one system occurs, our approach recalculates the criticalities of all dependent systems. In case of criticalities growth, when it goes through the diagonal of criticality matrix and reaches its margin values,

Figure 7. Example of obtaining new criticality matrixes, using influence matrixes



INITIAL CRITICALITY MATRIX

		Severity of failure mode		
		H	M	L
Failure rate	H	🟥	🟥 S_2	🟥
	M	🟥	🟨	🟨 S_3
	L	🟨 S_1^*	🟨	🟨

INFLUENCE MATRIX

	S_1	S_2	S_3
S_1	-	H	H
S_2	H	-	-
S_3	-	L	-

NEW CRITICALITY MATRIX

		Severity of failure mode		
		H	M	L
Failure rate	H	🟥	🟥 S_2^*	🟥 S_3
	M	🟥	🟨	🟨
	L	🟨 S_1^*	🟨	🟨

some actions should be taken to decrease criticality and improve the smart grid safety.

Example of obtaining new criticality matrices, using influence matrices, is shown on Figure 7.

Case – Study: Influence Analysis for Zaporozhe NPP

The influence values database might be completed for all Ukrainian NPPs considering their possible influences on the neighboring PG systems. This database might be very useful when assessing the consequences of NPP accidents for the power grid systems and vice versa. This database is constantly updated according to the Ukrainian power grid structure changing. The Ukrainian PG is divided in four zones according to the number of Ukrainian NPPs.

Table 4 represents a fragment of total influence values database completed for Zaporozhe NPP (ZNPP).

The similar influence matrices are built for each level of hierarchy of power grid criticality matrices.

The first stage is constructing an operational hierarchy of power grid criticality matrices without considering subsystem failures. The fragment of the operational hierarchy of power grid criticality matrices for Zaporozhe NPP is shown on Figure 8.

Criticality matrix $M_{crt}^{S_0}$ is completed for the power grid systems connected to Zaporozhe NPP (S1), where S2 stands for Dnipro Substation, S3 stands for Krivyi Rih TPP, S4 stands for Zaporozhe Substation, S5 stands for Kherson CHP. Criticality matrix $M_{crt}^{S_1}$ is completed for Zaporozhe NPP subsystems (power units, etc). Criticality matrix $M_{crt}^{S_1}$ is completed for Dnipro Substation subsystems, etc.

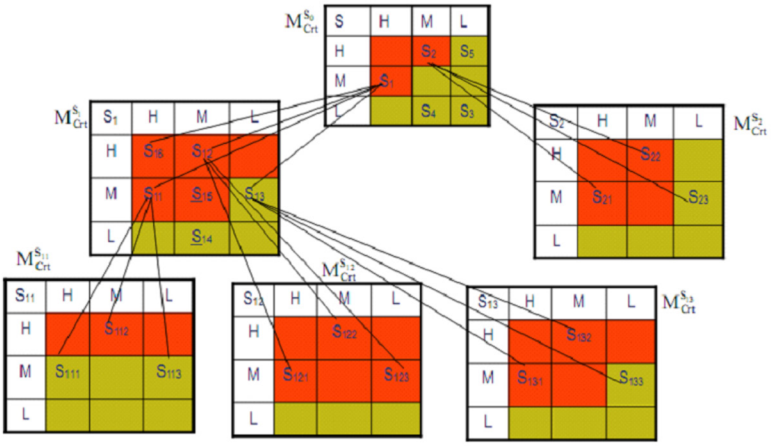
These power grid criticality matrices are regularly updated. Criticality values are calcu-

Table 4. Matrix of influence for Zaporozhe NPP

	Z NPP	Subst. Dnipro	Krivyi Rih TPP	Zapor. Subst.	Khersonska CHP
ZNPP	-	M	H	H	L
Subst. Dnipro	L	-	M	L	L
Krivyi Rih TPP	M	H	-		M
Zaporozhe Substation	M	M	M	M	M
Kherson CHP	L	L	L	M	L

where CHP is combined heat power station.

Figure 8. The fragment of the operational hierarchy of power grid criticality matrices for Zaporozhe NPP



lated considering the equipment parameter change. The criticalities for $M_{crt}^{S_0}$ are calculated as a sum of criticalities of the lower level hierarchy. The study for creating and implementing criticalities evaluation software is conducted by the researchers of the Centre of Safety Infrastructure-Oriented Research and Analysis, Ukraine. The system criticality change on each level of operational hierarchy determines the power grid safety trend.

The following stage of the power grid safety assessment is constructing the operational hierarchy of criticality matrices considering the occurrence of non-critical failures.

The shut down of the Zaporozhe NPP power unit 2 (2011) caused by the power grid disturbances was studied with constructing of the operational hierarchy of power grid criticality matrices. Any change of PG system operational mode could be considered a potential conditional event or risk factor as it was in Sayano-Shushenskaya HPP accident.

The incident involved only the second level hierarchy. The new operational hierarchy of criticality matrices considering the total influence matrix was constructed for NPP subsystem.

The total influence value for NPP subsystems considers not only the physical influence change, but also the organizational (through NPP unit load procedure) influence between NPP units.

The fragment of the operational hierarchy of PG criticality matrices after Zaporozhe NPP unit 2 shut down is shown on Figure 9.

As a result of the power unit shut down, the criticality of the power unit 3 was increased. The new criticality values were calculated considering the influence matrix constructed for the NPP subsystem. The new criticality values allow evaluating the new power grid safety value.

To understand the nature of influence between NPP and power grid we introduce the approach for formalization based on application the influence matrix. The influence formalization might be very useful NPP safety assessment. The influence might be useful for the risk analysis based on FMECA as the additional information to compare the possible failures criticalities. The conditional criticality complements the traditional criticality assessment and considers the mutual failures criticality changes. Using the different metrics we could evaluate the strength of influence. The

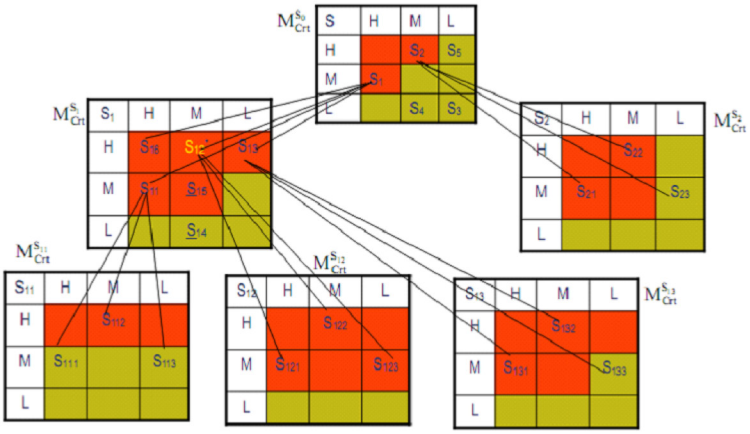


Figure 9. The fragment of the operational hierarchy of power grid criticality matrices after Zaporozhe NPP unit 2 shut down

principle of influence balance was suggested as one of principles of infrastructure safety assurance.

POWER GRID SAFETY: DYNAMICAL CRITICALITY CWW-BASED ANALYSIS

The PG is a huge and interconnected network composed of power-generation stations, high-voltage transmission lines, lower voltage distribution systems, and other support components. Disturbances in power grid operation can originate from natural disasters, failures, human factors, terrorism, and so on.

In its turn, the PG safety is stipulated by the NPP safety. Outages and faults will cause serious problems and failures in the interconnected power systems. Therefore, PGs require continuous control and balancing actions based on engineering systems.

It is of high priority to consider PG safety, mutual influence of NPP and PG systems and forecast possible accidents and failures considering their severity and high costs of recovery.

There are a lot of approaches and techniques of PG safety assessment. An approach to PG safety analysis, taking into consideration technical, organizational, and individual aspects, is proposed in (Linstone, 1984). The PG safety analysis is supplemented by a set of geographic and economic aspects in (Kaijser, 1984). An approach for PG safety assessment based on processing statistical data related to PG operation is proposed in (Holmgren, 2006). The main task of the safety statistical analysis is to determine the failure probability distribution function and to assess power grid risk. Lack of statistics prevents the use of traditional statistical methods for PG safety assessment.

Beside well known techniques of probabilistic and deterministic PG safety analysis there are a lot of approaches used for NPP safety assessment. Logic methods (Fault Tree Analysis and Event Tree Analysis), used for NPP safety analysis, are applied in (Bedford et al., 2001). Typical PG safety analysis techniques are connected with the equipment failure analysis, environment and human factor. Nowadays, a new type of grid hazards – intentional attacks occur. This type of hazards is analyzed by the use of probabilistic approach together with conditional probabilities calculation. However, mutual influence of systems, taking into account dynamical aspects of functioning and variation of risks caused by their failures, is not considered. Recently, network modeling has been revived due to computer technology progress and increase of interest in complex systems analysis. Achievements in a graph theory for complex systems analysis are reviewed in (Albert et al., 2002). A topology of North American Power System is analyzed. Graph is used as a model in (Albert et al., 2002). Evaluations, specifying Power System topology, lack of connectivity, while demounting vertexes that connect transmitting substations, are calculated. Two types of power grid safety hazards are analyzed: random failures and antagonistic (intentional) attacks.

There are no models that completely describe all power grid characteristics. Many models cover their technical aspect. The graph provides only conceptual view on power grids. It is used for cascading effect analysis without power flows consideration. In (Glass, 2005) it is specified that justification of failure preventive measures for power grid operation leads to its structure unimportance in comparison to operating modes. Large man-made disasters happen due to cascading failures.

Some methods used for PG safety analysis are qualitative and based on expert evaluations. Analysis results are represented in the form of risk matrix containing failure effect frequency and severity. Qualitative techniques of the safety analysis do not operate numeric data providing results as descriptions, recommendations. The safety assessment is related to a qualitative description of the frequency of undesired events, damage and threat scenario.

In (Moskalenko, 2010) it is specified that safety of a power grid can be improved by implementing of process automation in disturbance situations.

Generally, there is a lack of publications devoted to development of the power grid safety concept.

Common disadvantages of mentioned approaches are as follows:

- Power grid systems safety values are considered separately. The approaches considering NPP safety stay apart from approaches considering PG safety;
- Power grid safety is considered a static attribute;
- No consideration provided for mutual influences between power grid systems.

To assure the power grid safety, it is necessary to consider and thoroughly analyze the nature of interaction among power grid systems, including the NPP. The goal of the chapter is to introduce an approach to power grid safety assessment considering the different type of influence inside PG among its systems (in our case related to NPP). This technique can be useful to evaluate safety of NPP or PG taking into consideration their mutual influences.

PRINCIPLES AND TECHNIQUES OF DYNAMICAL CRITICALITY

CWW-Based Analysis

General Principles and Stages of Analysis

The technique represented in the chapter can be considered an essential part of PG risk management and can serve as a base for decision-making to avoid disturbances or minimize the severity of their consequences considering the interaction between NPP and PG systems.

The PG safety analysis is carried out taking into consideration principles of dynamism, hierarchy, uncertainty, and influence (interaction) of subsystems.

Principle of dynamical analysis assumes to record changes of system criticality during the operation as a result of changes of its states (transition to state of non-operability). At each stage of life cycle the criticality assessment specification and adjustment of criticality matrices (Kharchenko et al., 2009), taking into consideration probable changes, are carried out.

The *principle of hierarchy* assumes representation of grid structure as a hierarchy. The set of criticality matrices of subsystem failures groups in clusters.

The *principle of influence* of subsystem failures of i-level (on subsystem failure criticality of the same level) and influence on subsystems of (i-1)-level (higher) is important.

The safety of all influenced subsystems must be reconsidered.

The *principle of uncertainty* takes into consideration information incompleteness and uncertainty related to the conditions that cause PG accidents.

The stages of PG dynamical criticality CWW-based analysis are shown in Figure 10.

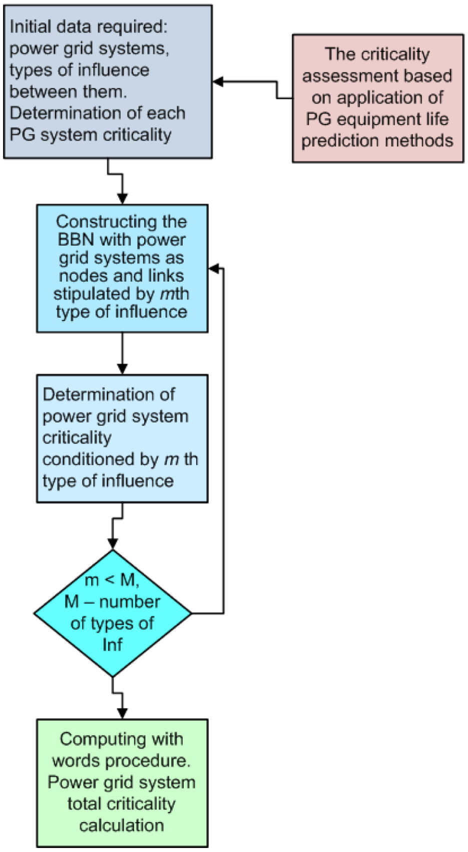
The power grid is a very complex system. It is characterized by huge number of nodes and links between nodes with increasing structural complexity; links between nodes could change over time, have different weights, directions, etc.

The safety is one of important attributes of PG. The PG safety is an integral value composed of grid systems safety values. The grid safety is determined by the uncontrolled mutual influence among grid systems. It is worth to note that influence exists on all grid levels and have to be taken into consideration when providing grid systems safety.

Types of Influences Between Power Grid Systems

According to the principle of influence, all influences (or relationships) existing in PG can be divided into several hierarchy levels. The influence is an ability of one PG system to determine the state, characteristics or processes in other systems. Any type of influence is a time dependent value. The changes in NPP state and characteristics stipulate the changes in the influence value.

Figure 10. The stages of power grid system' dynamical criticality CWW- based analysis


Initial data required: power grid systems, types of influence between them. Determination of each PG system criticality
The criticality assessment based on application of PG equipment life prediction methods
Constructing the BBN with power grid systems as nodes and links stipulated by *m*th type of influence
Determination of power grid system criticality conditioned by *m* th type of influence
m < M, M – number of types of Inf
Computing with words procedure. Power grid system total criticality calculation

The formalization of influences between PG systems is very helpful for its safety assessment and might be based on criticality matrices. For example, if PG system S_1 consists of three subsystems S_{11}, S_{12}, S_{13}, then criticality matrix, which represents the system S_1, might be presented as shown in Table 5.

According to the principle of hierarchy, the grid structure might be represented as a hierarchy. In this case the safety of PG systems of higher level hierarchy might be evaluated as a sum of criticalities of power grid systems of a lower

Table 5. Criticality matrix for system S_1

System S_1		Severity of failure mode		
		H	M	L
Failure rate	H		S_{12}	
	M			S_{13}
	L	S_{11}		

level hierarchy. For example, considering the criticalities of S_{11}, S_{12}, S_{13} as subsystems of S_1 its criticality could be calculated as:

$$Crt(S_i) = P(S_1) \times Sev(S_1) + P(S_2) \times Sev(S_2) + P(S_3) \times Sev(S_3) = \sum_i^I P(S_i) \times Sev(S_i). \tag{12}$$

It is suggested to treat criticality as power grid system's safety inverse index. The more system criticality the less its safety and vice versa.

It is worth to note that a probability of the system accident and its severity could be handled as a linguistic or numerical value. Hence, criticality is also treated correspondently either linguistic or numerical value.

The set of states Ω_{Si} of any PG system S_i is determined as:

$$\Omega_{Si} = \{\text{Crt}\ (S_i)=\text{High, Crt}\ (S_i)=\text{Medium, Crt}\ (S_i)=\text{Low}\}. \tag{13}$$

Any accident or failure of the power grid system leads to the change of criticality of all connected systems. When a failure of one system occurs, our technique recalculates the criticalities of all dependent systems.

The prognosis and assessment of PG system service life based on real time measurements will help to identify grid systems most likely to fail. The potential estimation methods and equipment service life prediction for complicated systems consist of deterministic, statistical, physical-statistical and methods based on expert knowledge. These methods are used to predict the probability of accident of any system S_{ij} of S_i.

This criticality assessment is used to support the subjective expert judgment on the initial power grid system state. The more system criticality calculated on (12) the more confident expert's opinion on the criticality of each node of PG.

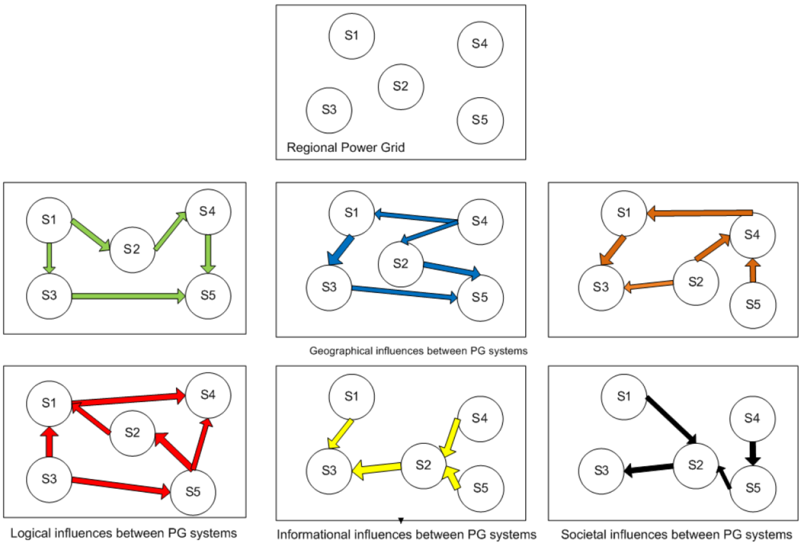
Bayesian Belief Network as a Model for Power Grid's Safety Assessment

The state of each PG system is determined by types of influence mentioned above. The Figure 11 represents the different types of networks, which characterize the same PG. Hence, all networks have the same nodes as PG systems, but different types of influence, which stipulate the different causal links between nodes. The different colors are used to show different types of influence (green – physical influence, blue – geographical, brown – organizational, red – logical, yellow – informational and black – societal). The different types of influence are characterized by its own weight. The more weight of the given type of influence the more sensitive PG's safety to this type of influence. Apparently the physical influence is more important, when PG safety is considered. But all types of influences should be taken to provide a more accurate PG safety evaluation. For each type of influence might be introduced its own type of PG system particular criticality. It means that PG could be more vulnerable to the change of one type of influence and at the same time be insensitive to other type influence change.

Considering the types of influence mentioned, it is assumed that the total PG system criticality is a function of power grid system's particular criticalities stipulated by the different types of influence, i.e.

$$Crt(S_i) = f(Crt^{org}(S_i), Crt^{fhys}(S_i), Crt^{geo}(S_i), Crt^{\log}(S_i), Crt^{soc}(S_i), Crt^{\inf}(S_i)) \tag{14}$$

Figure 11. Network of power grid systems with the different types of influences between them


S1
S2
S3
S4
S5
Regional Power Grid
Geographical influences between PG systems
Logical influences between PG systems
Informational influences between PG systems
Societal influences between PG systems

where $Crt\ (S_i)$ - the total power grid system criticality; $Crt^{org}(S_i)$ - particular criticality of power grid system conditioned by organizational influence in PG; $Crt^{fhys}(S_i)$ - particular criticality of power grid system conditioned by physical influence in PG; $Crt^{\log}(S_i)$ - particular criticality of power grid system conditioned by logical influence in PG; $Crt^{\inf}(S_i)$ - particular criticality of power grid system conditioned by informational influence in PG; $Crt^{soc}(S_i)$ - particular criticality of power grid system conditioned by societal influence in PG.

Depending on the scale used to evaluate criticality, each PG system could be characterized by the tuple of its criticalities values considering the types of influence, which determine these criticalities. Example of power grid system criticality tuple is shown in the Table 6.

The following task is to calculate the particular criticality stipulated by the given type of influence. We suggest using Bayesian belief networks (BBN) to evaluate the criticalities of the different PG systems.

BBNs are very effective for modeling situations, where some information is already known and incoming data is uncertain or partially unavailable (unlike rule-based or "expert" systems, where uncertain or unavailable data results in ineffective or inaccurate reasoning). These networks also offer

Table 6. Example of power grid system criticality tuple

Power Grid system	Type of influence					
	Physical	Informational	Geographic	Logical	Organizational	Societal
	Criticalities caused by the given type of influence					
PG system 1	H	H	M	L	L	L
PG system 2	H	M	M	L	L	H
………..						
PG system N	L	H	M	M	M	L

consistent semantics for representing causes and effects (and likelihoods) via an intuitive graphical representation. An important fact to realize about Bayesian belief networks is that they are not dependent on knowing exact historical information or current evidence.

According to approach it is suggested to construct BBN for each type of influence. Each node of BBN is represented by criticality matrix. Nodes are connected by links, which represent the different types of influence. We consider six types of influence among power grid systems.

Fragments of six BBNs are shown in Figure 12.

Hence, BBNs, which describe the PG system safety, consist of set of nodes. For each node the set of state is introduced. As mentioned above the state of node is characterized by value of its criticality calculated according to (12).

Every node also has a conditional probability table, or CPT, associated with it. Conditional probabilities represent likelihoods based on prior information or past experience. A conditional probability is stated mathematically as, i.e. the probabilities of the power grid system (child node), being at state characterized by expressions "Criticality is High (Medium, Low)" considering all possible combinations of other PG systems (parents' nodes) criticalities (High, Medium, Low).

Let us consider the fragment of BBN related to the informational influence between systems S_1 S_2 S_3, where the criticality of S_3 (child node) is conditioned by criticalities both of S_2 S_3 (parents' nodes).

Probability of $S_{3,}$ being at one of the established state Ω_{S3} depending on the states of parents nodes, could be determined as:

$$P(S_3^{(k)}) = \sum_i \sum_j P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)}) * P(S_1^{(i)}) * P(S_2^{(j)}), \tag{15}$$

where $P(S_3^{(k)})$ - the probability for S_3 being at k-th state; $P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)})$ - conditional probability for PG system S_3 to be at k-th state provided system S_1 being at i th state and system S_2 being at j –th state; $P(S_1^{(i)})$ - the probability for S_1 being at i-th state determined by expert taking into account value (12); $P(S_2^{(j)})$ - the probability for S_2 being at j-th state determined by expert taking into account value (12); .

In this case the probability for system S_1 being at the state described by expression "Criticality - High" is calculated as presented in Box 1.

The probabilities of S_1 being at the states described by expressions "Criticality – Medium" and "Criticality-High" are determined similarly.

The power grid system S_i state conditioned by the given type of influence is determined on the criterion:

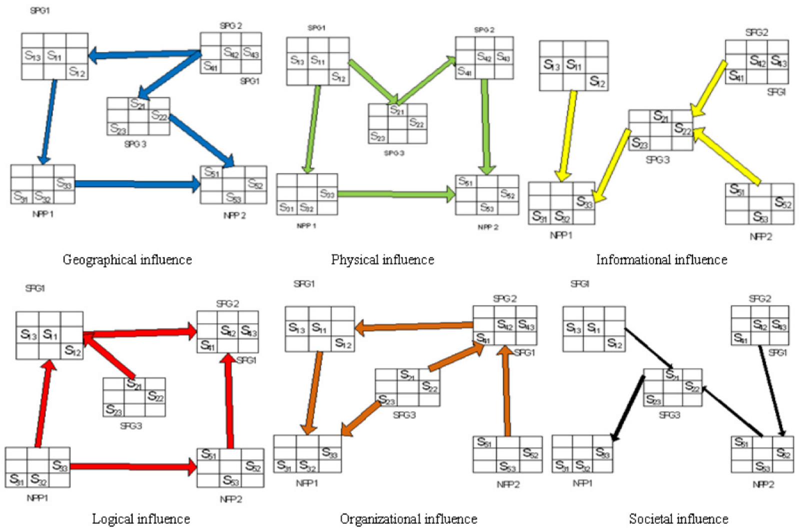
$$\begin{aligned} Crt(S_i) = \arg\max(P(Crt(S_i) = High), \\ P(Crt(S_i) = Medium), P(Crt(S_i) = Low), \end{aligned} \tag{17}$$

where $P(Crt(S_i) = High)$ – the probability of the power grid system of being at the state described by linguistic value High; $P(Crt(S_i) = Medium$ - the probability of the power grid system of being at the state described by linguistic value Medium; $P(Crt(S_i) = Low$ - the probability of the power grid system of being at the state described by a linguistic value Low. Similarly for each power grid system all criticalities, determined by different types of influence, are calculated and represented as power grid system criticality tuple shown in Table 6.

Analysis of the Linguistic Computational Models

The CWW is used to evaluate the total criticality for each power grid system.CWW procedure uses the linguistic assessments and make computations with them. Foundations and applications providing the current status of theoretical and

Figure 12. Fragments of six BBNs for different types of influence



empirical developments in CWW can be found in (Zadeh, 2001).

The linguistic approach based on fuzzy sets has given very good results for qualitative risk-analysis of critical information control system based on FMECA. It is an approximate technique in its essence, which represents qualitative aspects as linguistic values by means of linguistic variables, that is variables whose values are not numbers but words or sentences in a natural or artificial language.

The fuzzy linguistic approach deals with qualitative aspects that are represented in qualitative terms by means of linguistic variables. When a problem is solved using linguistic information, it implies the need for CWW. Here, an important limitation for this approach appears, because the computational techniques used in the specialized literature present a common drawback, the "loss of information," that implies a lack of precision in the final results.

These computational techniques are as follows. The first one is based on the extension principle (Brezhnev, 2010). It makes operations on the fuzzy numbers that support the semantics of the linguistic terms.

The second one is the symbolic method. It makes computations on the indexes of the linguistic terms.

In both approaches, the results usually do not exactly match any of the initial linguistic terms, then an approximation process must be developed to express the result in the initial expression domain. This produces the consequent loss of information and hence the lack of precision (Bowles, J. B., 2004).

As mentioned above many aspects of risk analysis process cannot be assessed in a quantitative form, but rather in a qualitative one, i.e., with vague or imprecise knowledge. In that case, a better approach may be to use linguistic assessments instead of numerical values. The variables, which participate in these problems, are assessed by means of linguistic terms. This approach is adequate in some situations, for example, when attempting to qualify phenomena related to human perception, we are often led to use words in natural language.

The use of linguistic assessments implies to make computations with them.

For example, a set of seven terms S could be given as follows:

S = {S_0: N, S_1: VL, S_2: L, S_3: M, S_4: H, S_5: VH, S_6: P}.

Usually, in these cases, it is required that the linguistic term set satisfies the following additional characteristics:

1. There is a negation operator, $Neg(s_i) = s_j$ such that j=g-I (g +1) is the cardinality).
2. $s_i \leq s_j \Leftrightarrow i \leq j$.

Therefore, there exists a minimization and maximization operator.

In this paper, we shall use labels with triangular membership function. For example, we may assign the following semantics to the set of seven terms (graphically, see Figure 13):

H = (0.5, 0.67, 0.83), VH = (0.67, 0.83, 1),

P = (0.83, 1, 1), VL=(0, 0.17, 0,33), L=(0.17, 0.33, 0.5), M=(0.33, 0,5, 0.67), N = (0, 0, 0.17).

Other authors use a nontrapezoidal representation, e.g., Gaussian functions (Holmgren, 2006).

The extension principle has been introduced to generalize crisp mathematical operations to fuzzy sets. The use of extended arithmetic based on the extension principle increases the vagueness of the results. The results obtained by the fuzzy arithmetic are fuzzy numbers that usually do not match any linguistic term in the initial term set, so a linguistic approximation process is needed to express the result in the original expression domain.

In the literature, we can find different linguistic approximation operators (Brezhnev, 2010).

A linguistic aggregation operator based on the extension principle acts according to

$$S^n \xrightarrow{\tilde{F}} F(R) \xrightarrow{app_1(\cdot)} S \text{ ,}$$

where S^n symbolizes the n Cartesian product of S, $\tilde{F}$ is an aggregation operator based on the extension principle, F(R) the set of fuzzy sets over the set of a real number R, app_1: F(R) → S is a linguistic approximation function that returns a label from the linguistic term S, whose meaning is the closest to the obtained unlabeled fuzzy number and S is the initial term set. Fuzzy sets C_j (the new values of criticality) are obtained by the means of fuzzy arithmetic for triangular fuzzy numbers. The fuzzy numbers characterize the semantic of linguistic values. Multiplication of two fuzzy numbers P (fuzzy probability) and L (fuzzy severity) may be obtained as $L \odot P \overset{def}{=} C$, where membership function equals

$$\mu_C = \sup_{\substack{x_1, x_2 \\ y = x_1 \cdot x_2}} \min \left\{ \mu_L(x_1), \mu_P(x_2) \right\}.$$

These new criticality values are fuzzy sets that do not exactly match any linguistic term in S, therefore, we must apply a linguistic approximation process based on the Euclidean distance to each C_j for obtaining the results in the initial term set

$$d(S_l, C_j) = \sqrt{P_1(a_l - a_j)^2 + P_2(b_l - b_j)^2 + P_3(c_l - c_j)^2} \text{ ,}$$

representing (a_l, b_l, c_l) and (a_j, b_j, c_j) the membership functions of "S_l" and "C_l" respectively. Being p_1, p_2, p_3 weights that measure the representativeness of the parameters *a, b, c* of the membership function of the fuzzy set. These weights satisfy:

$$P_i \in [0,1];$$

$$\sum_i P_i = 1.$$

Box 1.

$$\begin{aligned}
&P(Crt(S_3)=High))=\\
&P(Crt(S_3)=H\,/\,Crt(S_1)=H,Crt(S_2)=H)*P(Crt(S_1)=H)*P(Crt(S_2)=H)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=H,Crt(S_2)=M)*P(Crt(S_1)=H)*P(Crt(S_2)=M)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=H,Crt(S_2)=L)*P(Crt(S_1)=H)*P(Crt(S_2)=L)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=M,Crt(S_2)=H)*P(Crt(S_1)=M)*P(Crt(S_2)=H)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=M,Crt(S_2)=M)*P(Crt(S_1)=M)*P(Crt(S_2)=M)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=M,Crt(S_2)=L)*P(Crt(S_1)=M)*P(Crt(S_2)=L)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=L,Crt(S_2)=H)*P(Crt(S_1)=L)*P(Crt(S_2)=H)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=L,Crt(S_2)=M)*P(Crt(S_1)=L)*P(Crt(S_2)=M)+\\
&+P(Crt(S_3)=H\,/\,Crt(S_1)=L,Crt(S_2)=L)*P(Crt(S_1)=L)*P(Crt(S_2)=L).
\end{aligned} \tag{16}$$

Therefore, $app_1(\cdot)$ chooses S_l^* $(app_1(C_j)=S_l^*)$ such that, $d(S_l^*,C_j)\leq d(S_l,C_j)\,\forall S_l\in S$.

This linguistic process is applied to the above fuzzy sets, with P_1=0.2, P_2=0.6, P_3=0.2. According to these values, parameter "b_i" is the most representative of the membership function and "a_i" and "c_i" are equally representative.

The Figure 14 illustrates the geometrical interpretation of linguistic approximation, where the obtained fuzzy set (depicted as dashed line) and the closest fuzzy set (depicted in black).

HPP Accident Case Study Based on Dynamical Criticality CWW Analysis

To demonstrate the approach to the power grid safety analysis, using the dynamical criticality CWW analysis, Russian Sayano-Shushenskaya HPP failure (August, 2009) is considered. This HPP is one of the largest (together with Bratskaya HPP) used for power control of the whole power system with installed capacity - 6,4 mm kW, annual output - 22,8 bln kW p.h. Ten hydraulic units, each of 640 kW, are installed in the plant.

The BBN built for fragment of Siberian power systems. BBN's nodes are criticalities matrixes

Figure 13. A set of terms with its semantic

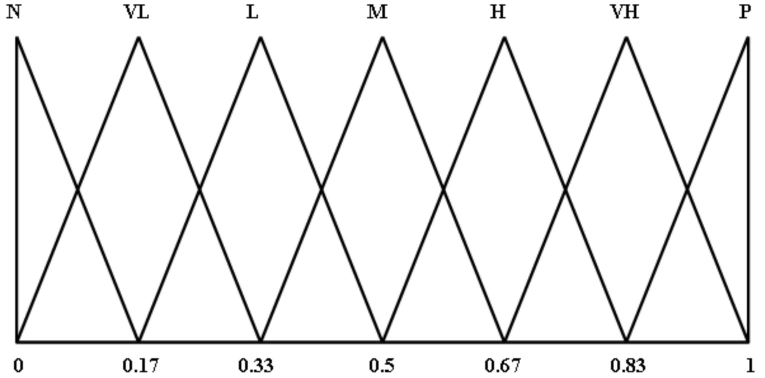
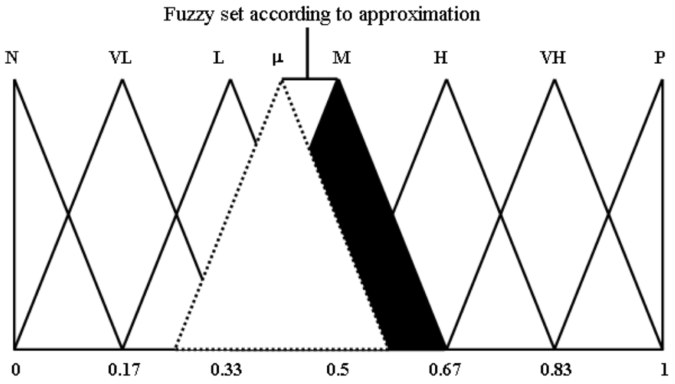


Figure 14. The geometrical interpretation of linguistic approximation



of Sayano–Shushenskaya HPP – S_1, Mayansk HPP – S_2, Bratskaya HPP– S_3, Thermal Power Plant (TPP) of Bratsk– S_4.

Fragment of BBN with Criticality matrixes as the nodes and links represented by physical influences constructed for Siberian power system is shown in Figure 15. The total criticalities of power grid systems before and "nearly to" accident are shown in Table 7 (Table 8). The sequential increasing of load from Bratskaya HPP and Mayansk HPP resulted to increasing the criticality of S_1, and finally led to destruction of HPU – 2 (S_{32}). Increasing of total criticality of S_1 led to increasing criticality of S_4.

The proposed technique may be applied to safety assessment of the power grid taking into account its systems influence. The technique is based on the use of the dynamical criticality matrices hierarchy. The power grid's capacity to predict the possible safety change could be improved by implementing of the decision making system. The technique suggested in the paper is considered as a part of this system. The power grid safety assessment is carried out taking into consideration principles of dynamism, hierarchy,

Figure 15. Fragment of BBN with Criticality matrixes as the nodes and links represented by physical influences constructed for Siberian power system

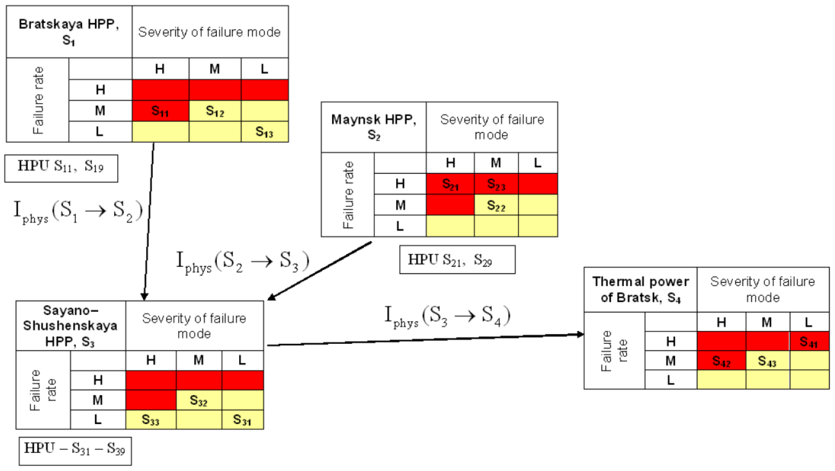


Table 7. Fragment of Siberian power systems criticality tuple (before accident)

Power Grid system	Type of influence				Total criticality
	Physical	Informational	Geographic	Organizational	
	Criticalities caused by the given type of influence				
Sayano–Shushenskaya HPP	M	L	L	L	H
Mayansk HPP	L	L	L	L	L
Bratskaya HPP	M	M	L	M	M
Bratsk TPP	L	H	L	L	M

Table 8. Fragment of Siberian power systems criticality tuple (nearly to accident)

Power Grid system	Type of influence				Total criticality
	Physical	Informational	Geographic	Organizational	
	Criticalities caused by the given type of influence				
Sayano–Shushenskaya HPP	H	M	L	H	H
Mayansk HPP	H	M	L	M	M
Bratskaya HPP	L	M	L	M	M
Bratsk TPP	L	H	L	L	M

uncertainty and mutual influence of systems. BBN is used to predict the particular criticality of the PG system conditioned by the given type of influence. CWW is suggested to determine the total PG system criticality. The proposed technique may be applied to the power grid safety analysis considering the different types of influences between NPP and other power grid systems. Results of the analysis may be used to determine effective safety management strategies.

Consideration of the difference types of influence allows improving the accuracy of PG safety value.

Next step of the technique enhancement will be related to consideration of Ukrainian NPP safety analysis taking into consideration the types of influences of the power grid and development of the decision making tool-based system.

APPROACH TO NPP SAFETY ASSESSEMENT COMBINING FUZZY MODELS AND BAYESIAN BELIEF NETWORKS UNDER UNCERTANTIES

The problem of NPP and its systems (as an example, NPP I&C systems) safety assessment is topical due to importance of current tasks. Thus, for example, NPP safe operation is critical for the strategy of country industrial development and the growth of welfare of its citizens. Fukushima-1 NPP accident showed that the CI reliability and safety level contributes to the public confidence in them, which in turn has a direct impact on the length of their life cycle, their modernization and reconstruction projects financing level. The set of input data used in the analysis of NPP safety includes:

- **Deterministic Data (D_d):** An information set giving a credible description of NPP (specifications, operating parameters and modes, systems composition and structure, etc.);

- **Statistical (Historical) Data (D_s):** Accumulated by observation of NPP systems parameters throughout their life cycle. Into this category reliability and safety characteristics, operating environment conditions, external systems fit. Many parameters (quantitative attributes) describing NPP operation processes are in fact random values (RV). The need to consider a number of random factors leads to stochastic uncertainty in safety assessment and assurance;
- **Linguistic Data (D_L):** *Represented as natural language expressions,* obtained from professional experts in this field. A part of information about NPP behavior, relationships of parameters of its operation and environment may be represented in the form of expert knowledge, which should also be taken into account in NPP safety assessment.

The problem of NPP safety assurance cannot be solved within the scope of one disciplinary approach. Use of any group of methods of risk analysis due to, for example, the expert's preferences, *leads to loss and/or disregard of a part of input data describing* NPP operation.

Consequently, in order to obtain a reliable estimate of NPP safety it is expedient to use all the above groups of input data (deterministic, statistical, linguistic).

The problem of NPP safety assessment cannot be solved within the scope of one disciplinary approach. Consequently, in order to obtain reliable safety values it is reasonable to use all the above groups of input data.

Analysis of literature shows a lack of attention given to the issues of development of approaches to integration of different safety assessment methods Thus, the work (Leech et al., 2008) suggests an idea to combine qualitative and quantitative methods. The main premise is that qualitative methods should prepare base data for quantitative methods.

The work (Johnson et al., 2008) offers the idea of "methodological triangulation" – an extended model of methods integration. The integration discussed allows receiving information as to the extent of the results obtained using different methods agree or disagree. A common limitation in the known works is a lack of methods compatibility analysis, analysis of integration techniques, scaling of input and output parameters, choice of results aggregation rules, etc.

Consequently, NPP safety assessment methods integration must ensure both validity check for results obtained and enhanced assessment validity as a result of maximum coverage of the whole set of input data by a minimum set of methods and information technologies used.

Fuzzy technologies are actively used for NPP safety assessment. Thus, for example, in nuclear industry *Fuzzy Logic and Intelligent Technologies intensively are applied for solving fuzzy control problems*, which cannot be solved using existing methods and approaches.

BBNs are also widely used in system safety assessment tasks characterized by uncertainty, imperfect knowledge, influence of a variety of random factors. Thus, e.g., BBNs are used as a basis for creation of the expert diagnostics system for NPP operators (Kang et al., 1999), for modeling complex industrial facilities (Weber et al., 2006), as well for evaluation of reliability and safety assessment in complex systems (Weber et al., 2001).

The aim of this chapter is to introduce an approach to series integration of CI safety assessment methods using integration of FL methods and BBNs under uncertainty.

Joint FL-BBN Assessment of NPP Safety

General approach. The suggested approach is based on the following assumptions:

- Any NPP may be represented as a collection of hierarchical layers of objects, and namely, systems components and elements;
- Any object in NPP may be represented as a BBN.

The NPP hierarchy is a basic premise for representation of its safety assessment integration methods architecture as hierarchy as well. This means that parameters of conditions of, e.g., elements are used as input data for components safety assessment. Further these assessments serve as input data for determining subsystems safety. In this way the safety assessment runs from the bottom to the top, from systems of the lowest hierarchy layer to systems of a higher layer. The system safety ois a function of safety of its subsystems, components and elements.

On the other hand, subsystem safety assessments may be unitized in prediction (diagnostics) of their components condition. In this case safety assessment runs from the top to the bottom from systems of the highest hierarchy layer to lower layer systems.

Consequently, both upward and downward integration of methods is possible. Such an integration of different methods results in compensation of insufficiency of data for models of higher level due to "excessive" data in another, lower hierarchy layer.

The hybrid safety assessment method suggested by this approach is given in Figure 16.

System criticality as a safety value. A high criticality $Crt(S_i)$ of a system corresponds to its marginal (pre-emergency) state, in which its further use is prohibited or inexpedient or its recovery to operable condition is not possible or expedient. The main distinction between the margin state in a reliability theory and a high criticality in the safety theory is consideration of system failure consequences in pre-emergency condition.

Criticality assessments may be represented on qualitative and quantitative scales. This paper considers linguistic criticality assessments. Thus, for example, criticality can be represented as linguistic variable with terms {High (H), Medium (M), Low (L)}.

An illustration of semantic interpretation of linguistic terms of criticality, condition, e.g., NPP reactor, is presented in Table 9.

Procedure. In order to apply the suggested approach one will need: to chose a test object (system), for which safety rating will be established, the result is determination of the child system for using BBN block; specify which systems define safe state of the test object; the result is determination of the parent system for using BBN block; determine components of the parent system and parameters of their states; the result is logic and linguistic model of the parent system for determining their safety rating in terms of parameters of components for FLI block.

1. **Fuzzy Logic Inference (FLI) Block:** (Bottom-up analysis) for NPP safety systems assessment on the basis of parameters of its components. In order for the block to solve problems it should have solved the subtask of selecting the most important system components, which condition defines system safety. The task of forming of a set of *informative (essential) parameters*, the values of which allow distinguishing system conditions, must be solved. The basic data are deterministic input data – parameters

Figure 16. Hybrid safety assessment method

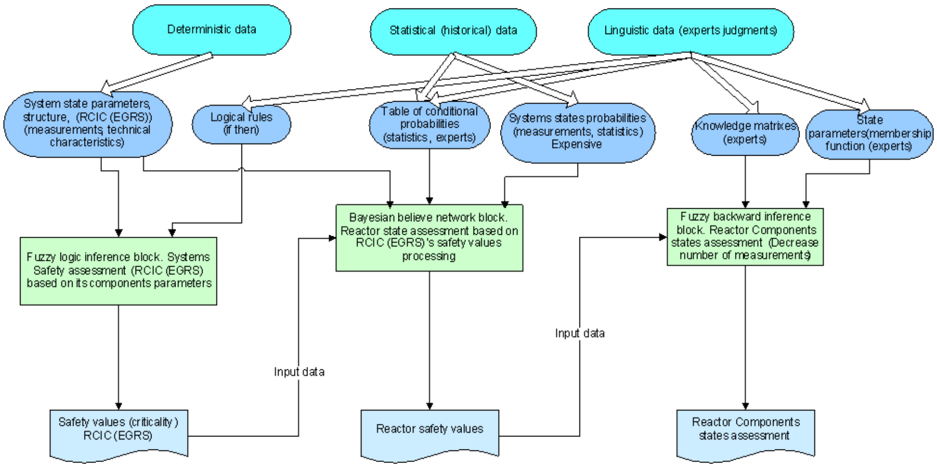

Deterministic data
Statistical (historical) data
Linguistic data (experts judgments)
System state parameters, structure, (RCIC (EGRS)) (measurements, technical characteristics)
Logical rules (if then)
Table of conditional probabilities (statistics, experts)
Systems states probabilities (measurements, statistics) Expensive
Knowledge matrixes (experts)
State parameters(membership function (experts)
Fuzzy logic inference block. Systems Safety assessment (RCIC (EGRS) based on its components parameters
Bayesian believe network block. Reactor state assessment based on RCIC (EGRS)'s safety values processing
Fuzzy backward inference block. Reactor Components states assessment (Decrease number of measurements)
Input data
Input data
Safety values (criticality) RCIC (EGRS)
Reactor safety values
Reactor Components states assessment

Table 9. Semantic interpretation of linguistic terms of systems criticality (reactor case study)

Reactor safety levels	Physical State Description
Criticality state – **HIGH** (reactor emergency state)	Uncontrolled power increase in the reactor core (heat generation), decreased coolant consumption (heat removal) and increased pressure in the primary coolant circuit. Reactor parameters are close to the rated values. For fuel elements these are fuel temperature, cladding temperature, burnout ratio, temperature of physical and chemical processes, heat flow. For the circuit these are pressure, temperature, brittle fracture ratio, pressure differentials
Criticality state – **MEDIUM** (Reactor pre-emergency state)	The state of unstable equilibrium of the reactor. The reactor is in a state of physical and thermohydraulic stability, which can be upset even by slight disturbances
Criticality state – **LOW**	Normal routine mode of reactor operation

of components operation. Output data are criticality condition of the system.

2. **BBN Block for CI safety Assessment:** The set of NPP systems is divided into two sets: parent and child systems. When using BBN parent systems, criticality conditions are used for determining criticality of the child systems. The basic data are parameters of criticality conditions of the parent systems obtained in the FLI block and conditional probability table (CPT). CPT determines the relation between system conditions. Probabilities can be represented on absolute and fuzzy scale. Input data are criticality condition of the child system.
3. **Fuzzy Backward Chaining Block:** To obtain predictive estimates of condition parameters of child system components. Probability distribution of estimates of child system criticality obtained using BBN is used as input data to derive logic equations. Additional information is the expert knowledge matrix R. The block's output data is predictive estimates of component conditions.

Application of FL-BBN Method for NPP Reactor Safety Assessment

FLI block application. NPP reactor safe condition is a function of a number of systems. Let us focus on the Reactor Core Isolation Cooling (RCIC) System and the Emergency Gas Removal System (EGRS) as an illustrative example. Importance of these systems for safe reactor condition was clearly demonstrated by NPP accidents. Their condition and reliable operation are critical for reactor safety.

RCIC is the first parent system for the reactor in terms of BBN (child system). It is designed for core emergency cooling. It is comprised of three interrelated systems: primary, back-up and continued cooldown subsystems.

EGRS is the second parent system, which performs the function of noncondensable gases removal from the first circuit, protects fuel elements, prevents natural circulation failure in the first circuit.

Consider the use of the FLI block to assess the criticality state of the RCIC.

The RCIC safety assessment task is represented as the task to find a representation in the following form:

$$X^* = (x_1^*, x_2^*, x_3^*, ..., x_n^*) \to d_j \in D = (d_1, d_2, d_3, ..., d_m),$$

where X^* – a set of parameters describing the state of RCIC components; D – a set of probable $d_j,\ j = \overline{1, m},$ RCIC safety values.

The first subtask of the block is to choose the set of components that are most important in terms of RCIC core cooling performance. For example, pumps, the condenser can be treated as such components. Reliable operation of any of the pumps is the critical aspect from the viewpoint of RCIC safety functions.

The second subtask of the block is to select functional parameters $x_1 \div x_n$ that evaluate the states of important RCIC components. Among critical parameters that evaluate pump stare are feed (F), pressure (P), rate of revolution (RR), water reserve in the condenser (C), etc. Increase (decrease) in these parameters with respect to certain values may be an indication of malfunctions or failures resulting in RCIC safety function degradation.

In this way, in order to assess RCIC safety it is necessary:

- to determine values of parameters describing RCIC components functioning

$$X^* = (x_1^*, x_2^*, x_3^*, ..., x_n^*)\ ;\ (18)$$

- to plot diagrams of RCIC safety linguistic terms membership function $\mu^{a_i^{jp}}(x_i^*)$;
- to determine values of the membership function $\mu^{a_i^{jp}}(x_i^*)$ at fixed values of parameters $X^* = (x_1^*, x_2^*, x_3^*, ..., x_n^*)$;
- using logic equations in the following form:

$$\mu^{d_m}(x_1, x_2, ..., x_n) = \mu^{a_1^{m1}}(x_1) \wedge \mu^{a_2^{m1}}(x_2) \wedge ....\mu^{a_n^{m1}}(x_n) \vee \mu^{a_1^{m2}}(x_1) \wedge ...$$
$$\wedge \mu^{a_2^{m2}}(x_2) \wedge \mu^{a_n^{m2}}(x_n) \vee ... \vee \mu^{a_1^{mk_m}}(x_1) \wedge \mu^{a_2^{mk_m}}(x_2) \wedge ... \wedge \mu^{a_n^{mk_m}}(x_n),$$
$$\vee - \log ical\ OR, \wedge - \log ical\ AND, \quad (19)$$

to determine values of membership functions for all possible RCIC safety values.

A knowledge base used to derive logic equations for RCIC is presented in Table 10.

Within the scope of the example, the logic equations are of the form:

$$\mu_{Y_1}(Crt = High) = [0.12 \wedge 0.55 \wedge\ 0.7 \wedge\ 0.66] \vee [0.12 \wedge 1.0 \wedge 0.7 \wedge 0.66] \vee [0.12 \wedge 1,0 \wedge\ 0.87 \wedge\ 0.66] = 0.12;$$

Table 10. RCIC knowledge base

Feed	Pressure	Rate of revolution	Condenser water reserve	RCIC criticality values
L	L	L	L	H
L	M	L	L	H
L	M	M	L	H
L	M	M	M	M
....				
H	H	M	H	L

$\mu_{Y_1}(Crt = Medium) =$[0.12 $\wedge$ 1.0 $\wedge$ 0.87 $\wedge$ 0.91] $\vee$ [0.87 $\wedge$ 0.55 $\wedge$ 0.87 $\wedge$ 0.66] $\vee$ [0.94 $\wedge$ 0.55 $\wedge$ 0.87 $\wedge$ 0.91]=0.55;

$\mu_{Y_1}(Crt = Low) =$ [0.87 $\wedge$ 1.0 $\wedge$ 0.87 $\wedge$ 0.91] $\vee$ [0.94 $\wedge$ 0.66 $\wedge$ 0.53 $\wedge$ 0.55] $\vee$ [0.94 $\wedge$ 0.66 $\wedge$ 0.53 $\wedge$ 0.91]=0.87.

Select d_j^* as a solution, for which,

$$\mu^{d_t^*}(x_1, x_2, ..., x_n) = \max[\mu^{d_j}(x_1, x_2, ..., x_n)],\ j = \overline{1, m},\ t = \overline{1, m}. \quad (20)$$

Criticality state of EGRS is determined in a similar manner. EGRS safety estimates are determined in the FLI block in terms of parameters of its components (excess steam-gas mixture removal bypass conduit, bypass conduit steam-gas mixture signal indicator, steam-gas pressure chamber).

BBN block application. The complex of systems including the reactor (child system) and RCIC and EGRS (parent systems) can be represented in the form of BBN.

This approach uses BBN for:

- Reactor criticality condition prediction according to the state of parent systems (RCIC and EGRS). This involves recalculation of a probability of the reactor child system being in each of its possible criticality conditions depending on incoming BBN parent systems condition change evidence using the CPT;
- Determination of conditions of the parent systems (RCIC and EGRS) according to evidences (facts) of their possible condition (diagnostics task).

In BBN probabilities of the reactor being (S_3) in different conditions of set S_3 depending on conditions of the parent systems (RCIC-S1, EGRS- S_2) can be determined by the relation of the following form:

$$P(S_3^{(k)}) = \sum_i \sum_j P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)}) * P(S_1^{(i)}) * P(S_2^{(j)}) \quad (21)$$

where $P(S_3^{(k)})$ - probability of S_3 being in k-*th* condition; $P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)})$ - a conditional probability of S_3 system in k-*th* condition given that S_1 system is in i-*th* condition and S_2 system in j-*th* condition. Conditional probabilities for BBN are set by professional expert; $P(S_1^{(i)})\,(P(S_2^{(j)}))$ - probability of $S_1(S_2)$ system being in i-*th* (j-*th*) condition.

This approach predicts reactor safety state without additional measurements of reactor parameters (pressure, temperature, etc.).

The block's output data are reactor safety predictive estimate represented in the form of the following probability distribution:

$P(Crt(R) = High)) = 0,6; P(Crt(\mathrm{R}) = Medium))$
$= 0,3; P(Crt(R) = Low)) = 0,1.$

The choice of reactor safety assessment is made according to the *maximum probability criterion*. Reactor condition assessment is a complex and costly task. Fukushima-1 accident proved the importance of the need for the reliable operation of monitoring systems (detectors). These risks can lead to a situation, when the operator can completely loose the sense of what is happening to the reactor. For support and decision making in case of station black-out it is necessary to use all the information (including indirect information) for reactor state assessment. Consequently, it is important to solve the problem of predicting reactor components condition without any measurement and using additional information. This task is solved in the fuzzy backward chaining block. A primary importance of fuzzy backward chaining is that it considers parameters, which are essential for safety, though physical measurement of which is substantially limited.

Fuzzy Backward Chaining Block for Prediction of Reactor Components Condition Parameters

The problem of fuzzy backward chaining lies in evaluation of input parameters describing reactor components condition, provided that the matrix of knowledge and reactor safety and output estimations are known.

In terms of input A and output B sets link between them can be represented in the following form $B = A \circ R$, where A(B) - a fuzzy set of input (output) parameters specified in space X(Y).

Matrix of knowledge R can be represented as

$$M_P = \begin{vmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \dots & \dots & r_{ij} & \dots \\ r_{m1} & r_{m2} & \dots & r_{mn} \end{vmatrix},$$

where r_{ij} – an element of matrix expressing the expert's confidence level in existence of cause-and-effect relations between a component input parameter and a corresponding output parameter describing safety of the system.

Considering BBN block the following distribution was obtained:

$P(Crt(R) = High)) = 0,7; P(Crt(\mathrm{R}) =$
$Medium)) = 0,1; P(Crt(R) = Low)) = 0,2.$

Introduce parameters conditions vector y_1, y_2, y_3. These parameters are values of the vector of the criticality probability distribution (BBN output parameters).

State this vector in the following form:

$$B = 0,7\big|y_1 + 0,1\big|y_2 + 0,2\big|y_2 .$$

In the fuzzy backward chaining block the expression, for example, $0,1\big|y_2$ means that the level of the expert's confidence that the system is in a certain condition $Crt(S_1) = Medium$ is equal to 0.1.

It is necessary to find such a fizzy set $A = \{\mu(x_1)\big|x_1,\ \mu(x_2)\big|x_2, \dots, \mu(x_n)\big|x_n\}$, that would correspond to fuzzy set B. Fuzzy set A can be represented as a vector $a = (a_1, a_2, \dots, a_n)$, where a_n – corresponding value of membership degree $\mu(x_n)$ of the reactor components condition parameter.

In this example reactor components are fuel elements S_{11} and circuit S_{12}. Two parameters a_1 – fuel element temperature and a_2 - pressure in the circuit are considered.

Examination results are presented as a knowledge matrix in the following form:

$$R = \begin{vmatrix} 0{,}9 & 0{,}1 & 0{,}2 \\ 0{,}6 & 0{,}5 & 0{,}5 \end{vmatrix}.$$

Considering the knowledge matrix and probability distribution in view of BBN the following logic equation was produced:

$$\begin{bmatrix} 0{,}7 & 0{,}1 & 0{,}2 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \end{bmatrix} \circ \begin{vmatrix} 0{,}9 & 0{,}1 & 0{,}2 \\ 0{,}6 & 0{,}7 & 0{,}5 \end{vmatrix}.$$

When using max-min compositions, the latter relation rearranges to the following form:

$$\begin{aligned} 0{,}7 &= (0{,}9 \wedge a_1) \vee (0{,}6 \wedge a_2) \\ 0{,}1 &= (0{,}1 \wedge a_1) \vee (0{,}7 \wedge a_2) \\ 0{,}2 &= (0{,}2 \wedge a_1) \vee (0{,}5 \wedge a_2) \end{aligned}$$

Solution of this equation produces the following values: $a_1 = 0{,}7; 0 \le a_2 \le 0{,}1$.

In this way, reactor condition obtained using BBN is influenced by a high temperature of fuel elements, since it is the premise that corresponds to the highest value of membership function.

Solution and Recommendations

No doubts the problem of the safe interaction between NPP and a PG is topical. In the future they will be connected together forming a very complicated and dynamical system of systems (SoS). To make this highly interconnected SoS safe and reliable the development of safety assessment technique and tool are required. Beside this we have to take into account the future trend of development of both of them. Smart grid is the future power grid which combines a traditional PG with an “intelligent” information and communications technology (ICT) infrastructure to create a smart power system. Undoubtedly, in the future NPPs will be an essential and integral part of smart grid. To assure the NPP safety, it is necessary to consider and thoroughly analyze the nature of interaction among smart grid systems and a nuclear power plant.

Next important steps of research and development activities, related to assurance of safety of NPP is to develop an approach which allows considering the new risks caused by smart grid vulnerabilities and their influences on NPP safety.

FUTURE RESEARCH DIRECTIONS

Future R&D are the following:

- The formalization of stability of the NPP-PG system and determination the balance of influences between its elements with application of economic balance theory;
- Development of the expert system to support the decision making process of operator under severe conditions;
- Development of tool which supports the FMECA-based approach for power grid criticality assessment;
- Smart grid and NPP risks assessment. Security issues of smart grid which can undermine the safety of NPP.

Beside all mentioned above this approach shall take into account the information technologies, which - on the one hand, can decrease the risks that attend NPP-PG interaction, but on the other hand, failures of computer-based decision making systems can cause additional safety deficits. We’ll consider the mutual influence between smart grid and NPP.

CONCLUSION

The complex nature of NPP and PG mutual interaction calls for the need of development of new approaches to NPP and power grid safety assessment. The chapter considers an approach to influences formalization and series integration of safety assessment methods as well. Two integration architecture types are introduced: series integration and parallel. The series integration might be useful to increase the safety values' validity. The parallel integration allows reducing the amount the safety – related information. Integration of BBN and FL allows capturing all available information required for safety assessment of complex dynamic system under uncertainties. Application of FL methods, when all parameters describing the system operation are known, allows determining the criticalities of all systems under interests. But for complex dynamical systems the processes of parameters' measurement might technically difficult. Application of BBN allows decreasing the amount information. Thus, for example, for FL-based safety assessment of reactor, RCIC and EGRS it is required to measure all parameters of all systems. Integration of FL-based methods and BBNs allows decreasing the amount of input information (measurements) and not measure reactor parameters. RCIC and EGRS parameters are only required. Thus, in the scope of the example this integration decreases on tierce of required information. This approach might be considered as a basis for the expert system to help the operator make the decisions, when I&C ability to measure the critical parameters is compromised due to the NPP blackout.

REFERENCES

Albert, R., Albert, I., & Nakarado, G. L. (2004). Structural Vulnerability of North American Power Grid. *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, *69*, 23–27. doi:10.1103/PhysRevE.69.025103

Albert, R., & Barabasi, A.-L. (2002). Statistical Mechanics of Complex Networks. *Reviews of Modern Physics*, *74*, 23–26. doi:10.1103/RevModPhys.74.47

Babeshko, E., et al. (2009). Extended dependability analysis of information and control systems by FME(C)A-technique: Models, procedures, application. In Proceeding of IEEE DepCoS RELCOMEX Conference. IEEE.

Bedford, T., & Cooke, R. M. (2001). *Probabilistic Risk Analysis: Foundation and Methods*. Cambridge, England: Cambridge University Press. doi:10.1017/CBO9780511813597

Bowles, J. B. (2004). An assessment of PRN prioritization in a failure modes effects and criticality analysis. *Journal of the IEST*, *47*, 45–54.

Brezhnev, E. (2010) Risk-analysis in critical information control system based on computing with words' model. *The 7th International Workshop on Digital Technologies, Circuit Systems and Signal Processing (pp.67-72), Zilina: University press.*

Brezhnev, E., & Kharchenko, V. etc (2011). Dynamical and Hierarchical Criticality Matrixes-Based Analysis of Power Grid Safety. *International Topical Meeting on Probabilistic Safety Assessment and Analysis (pp. 1137-1149), Wilmington.: ANS PSA 2011.*

Donald, D. Dudenhoeffer etc CIMS: A framework for infrastructure interdependencies and analysis. *The 2006 Winter Simulation Conference (pp.478-485), Washington: on CD.*

Gilchrist, W. (1998). Modeling failure modes and effects analysis. *International Journal of Quality & Reliability Management*, *10*(5), 16–23.

Glass, R. (2005). Simulation and Analysis of Cascading Failure in Critical Infrastructure. Working Together: R&D Partnerships in Homeland Security (pp. 45-56), Boston.

Holmgren A., Molin S. (2006) Using Disturbance Data to Assess Vulnerability of Electric Power Delivery Systems. *Journal Infrastructure systems, American Society of Civil Engineers (ASCE), 12 (4), 243-251.*

Johnson, B., & Christensen, L. (2008). *Educational research: Quantitative, qualitative, and mixed approaches*. Thousand Oaks, CA: Sage Publications. doi:10.1093/swr/32.1.3

Kaijser, A. (1984). *The Swedish Infrastructure – Historical Development and Future Challenges*. Stockholm: Carlsson.

Kang C·, Golay M (1999). Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. *Expert Systems with Applications, 17 (1), 21–32.*

Leech, N., & Onwuegbuzie, A. (2008). Qualitative data analysis: A compendium of techniques for school psychology research and beyond. *School Psychology Quarterly*, *23*, 587–604. doi:10.1037/1045-3830.23.4.587

Linstone, H. (1984). Multiple Perspectives for Decision-Making: Bridging the Gap Between Analysis and Action, Holland, Amsterdam.

Moskalenko, N., & Sokolnokova, T. (2010). Smart Grid – German and Russian Perspectives in Comparison. *International Conference on Modern Electric Power Systems 2010, (pp.23-30), Wroclaw, Poland*

ADDITIONAL READING

Reactor Safety Study – An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants, *WASH-1400 (NUREG-75/014), October 1998.*

Severe Accident Risk Assessment for Five U.S. Nuclear Power Plants, *NUREG-1150, Draft 2, 1989.*

The Ukrainian electricity system – a brief overview *(differgroup.com, February, 2012)*

Tsarenko, A. Viachaslau Herasimovich. (2008). Overview of Electricity Market in Ukraine. Center for Social and Economic Research – CASE Ukraine. – Kiev.

Weber, P., & Iung, B. (2001). System approach-based Bayesian Network to aid maintenance of manufacturing process. *6th IFAC Symposium on Cost Oriented Automation, Low Cost Automation. Berlin, Germany, October 8-9, 33-39 p.*

Weber, P., Jouffe, L. (2006). Complex system reliability modeling with Dynamic Object Oriented Bayesian Networks (DOOBN). Reliability Engineering and System Safety. - 1999. - Volume 91, Issue 2, 149-162 p.

Zadeh, L., & Kacprzyk, J. (2001). Computing with words in Information. Intelligent Systems – Part 1: Foundation, Part 2, USA.

KEY TERMS AND DEFINITIONS

Bayesian Belief Network: A probabilistic graphical model (a type of statistical model) that represents a set of random variables and their conditional dependencies via a directed acyclic graph (DAG).

Electrical Grid: An interconnected network for delivering electricity from suppliers to consumers. It consists of generating stations that produce electrical power, high-voltage transmission lines that carry power from distant sources to demand centers, and distribution lines that connect individual customers.

Fuzzy Logic: a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact. Compared to traditional binary sets (where variables may take on true or false values) fuzzy logic variables may have a truth value that ranges in degree between 0 and 1.

Probability (or Likelihood): A measure or estimation of how likely it is that something will happen or that a statement is true.

Smart Grid: A modernized electrical grid that uses information and communications technology to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity.

System Influence: The ability of one system to determine the state of other system.

System of Systems: a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems.

Compilation of References

Kang C·, Golay M (1999). Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. *Expert Systems with Applications*, *17 (1), 21–32.*

Abrial, J.-R. (2010). *Modeling in event-B*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9781139195881

Adamov, E. O. et al. (2005). *Nuclear engineering: Encyclopedia*. Moscow: Mashinostroenie.

Adziev, A. V. (1998). Myths about software safety: Lessons of famous disasters. Open systems, 1998, vol. 6. Retrieved December 16, 2012, from http://www.osp.ru/os/1998/06/179592/

Afanasyev, N., Belohin, O., Brenman, O., et al. (2002). Maintenance and safety assessment of computer information system of NPP unit with WWER-1000 reactor. *Nuclear and Radiation Safety, 4*.

Aizenberg, A., & Yastrebenetsky, M. (2002). Comparison of safety management principles for control systems of carrier rockets and nuclear power plants. *Space Science and Technology*, *1*, 55–60.

Albert, R., Albert, I., & Nakarado, G. L. (2004). Structural Vulnerability of North American Power Grid. *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, *69*, 23–27. doi:10.1103/PhysRevE.69.025103

Albert, R., & Barabasi, A.-L. (2002). Statistical Mechanics of Complex Networks. *Reviews of Modern Physics*, *74*, 23–26. doi:10.1103/RevModPhys.74.47

Anderson, R. B. (1979). *Proving Programs Correct*. New York: Wiley.

Anikanov, S., Bezsalyj, V., Belohin, O., et al. (2003). Maintenance and safety assessment of nuclear power plant safety parameters display systems of WWER-1000 reactor. *Nuclear and Radiation Safety, 1*.

Anikanov, S., et al (2003). Assurance and safety assessment of safety parameters display systems on NPP units with WWER-1000 reactors. *Nuclear and Radiation Safety,* (1).

ANSI/ISA-99.00.01-2007. (2007). *Security for industrial automation and control systems: Terminology, concepts, and models*. (IEEE 982.2, 1988)

ANSI/ISA-99.00.02-2007. (2007). *Establishing an industrial automation and control systems security program*. (IEEE 982.2, 1988)

ANSI/ISA-99.00.03-2007. (2007). *Operating an industrial automation and control systems security program*. (IEEE 982.2, 1988)

ANSI/ISA-99.00.04-2007. (2007). *Specific security requirements for industrial automation and control systems*. (IEEE 982.2, 1988)

ANSI/ISA-99.02.01-2009. (2009). *Security for industrial automation and control systems: Establishing an industrial automation and control systems security program*. (IEEE 982.2, 1988)

ANSI/ISA-TR99.00.01-2007. (2007). *Security technologies for industrial automation and control systems*. (IEEE 982.2, 1988)

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, *1*, 11–33. doi:10.1109/TDSC.2004.2

Babeshko, E., et al. (2008). Applying F(I)MEA-technique for SCADA-based industrial control systems dependability assessment and ensuring. In *Proceedings of International Conference on Dependability of Computer Systems DepCoS–RELCOMEX 2008*. Academic Press.

Babeshko, E., et al. (2009). Extended dependability analysis of information and control systems by FME(C)A-technique: Models, procedures, application. In *Proceeding of IEEE DepCoS RELCOMEX Conference*. IEEE.

Babeshko, E., et al. (2010). Approaches to NPP I&C systems dependability assessment: Analysis and implementation. In *Proceedings of International Congress on Advances in Nuclear Power Plants* (ICAPP. '10). ICAPP.

Babeshko, E. et al. (2011). Combined implementation of dependability analysis techniques for NPP I&C systems assessment. *Journal of Energy and Power Engineering*, *5*(42), 411–418.

Bachmatch, E., Marshevsky, M., Rozen, Y., et al. (2008). Assurance and safety assessment of fire-alarm systems and automatic fire extinguishing in the accommodations NPP. Nuclear and Radiation Safety, 1.

Bachmatch, E., Vinogradska, S., Rozen, Y., et al. (2005). The software-hardware complexes for the power automatic regulation, reactors power reduction and limitation and acceleration preventive protection: the safety insurance and assessment. Nuclear and Radiation Safety, 1.

Badrignans, B. et al. (2011). *Security trends for FPGAS: From secured to secure reconfigurable systems*. Berlin: Springer. doi:10.1007/978-94-007-1338-3

Bakhmach, E., Kharchenko, V., Siora, A., Sklyar, V., & Tokarev, V. (2009). Advanced I&C Systems for NPPS Based on FPGA Technology: European Experience. Paper presented at the meeting of the *17th International Conference on Nuclear Engineering, Belgium.*

Bakhmach, E., Siora, A., Bezsalyi, V., & Yastrebenetsky, M. (2008). Digital systems for reactor control: design, experience of operation. In *Proceedings of the 16th International Conference on Nuclear Engineering.* Orlando, FL: ICONE16.

Barkalov, A. et al. (2006). *Design of control units with programmable logic*. University of Zelena Gura.

Bashlykov, A. (1986). *Designing of decision-making systems in power engineering*. Moscow, Russia: Enrgoatomizdat.

Bedford, T., & Cooke, R. M. (2001). *Probabilistic Risk Analysis: Foundation and Methods*. Cambridge, England: Cambridge University Press. doi:10.1017/CBO9780511813597

Beliy, E. et al. (2008). Infomedia development concept in the state scientific and technical centre for nuclear and radiation safety. *Nuclear and Radiation Safety*, *2*, 59–68.

Belohin, O., Brenman, O., Kudinov, Yu, et al. (2007). Reconstruction of computer information system of South-Ukrainian NPP. unit 2. *Nuclear and Radiation Safety, 1*.

Belohin, O., et al. (2010). *Automatic control system of diesel-generator for NPP: Emergency supply*. Westron. Retrieved from http://www.westron.kharkov.ua/SAU_RDES.pdf

Ben-Ari, M. (2000). *Understanding programming languages*. Wiley.

Bessalov, G. et al. (2004). *Middle power WWER reactors*. Moscow: Akademkniga.

Biscoglio, I., & Fusani, M. (2010). Analyzing quality aspects in safety-related standards. In Proceedings of Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010. Las Vegas, NV: American Nuclear Society.

Bobrek, M., Bouldin, D., Holkomb, D., et al. (2009). Review guidelines for FPGAs in nuclear power plants safety systems. NUREG/CR-7006 ORNL/TM-2009/020.

Bouard, J.-P. (2002). International standardization in nuclear I&C engineering. In Proceedings of CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems. AEN/NEA.

Bowles, J. B. (2004). An assessment of PRN prioritization in a failure modes effects and criticality analysis. *Journal of the IEST*, *47*, 45–54.

Brenman, O., Denning, R., et al. (2006). Licensing review of foreign I&C systems for Ukrainian nuclear power plants. In Proceedings of International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies-5. Albuquerque, NM: Academic Press.

Brenman, O., et al. (2006). Licensing review of foreign I&C systems for Ukrainian power plants. In *Proceedings of International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies* (NPIC&HMIT 2006). Albuquerque, NM: NPIC & HMIT.

Brezhnev, E. (2010) Risk-analysis in critical information control system based on computing with words' model. *The 7th International Workshop on Digital Technologies, Circuit Systems and Signal Processing (pp.67-72), Zilina: University press.*

Brezhnev, E., & Kharchenko, V. etc (2011). Dynamical and Hierarchical Criticality Matrixes-Based Analysis of Power Grid Safety. *International Topical Meeting on Probabilistic Safety Assessment and Analysis (pp. 1137-1149), Wilmington.: ANS PSA 2011.*

Bukowsky, J., & Goble, W. (1994). An Extended Beta Model to Quantize the Effects of Common Cause Stressors. Paper presented at the meeting of the *ISAFECOMP, London.*

CISPR. (2006). CISPR 22 . Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement.

Cluley, J. C. (1994). *Reliability in instrumentation and control*. London: Butterworth Heinemann.

Cox, M., & Shumov, S. (2011). About activities of IEC/TC45 nuclear instrumentation. Nuclear Measurement and Information Technologies, 3(35).

Didenko, K., & Rozen, Y. (1985). MikroDAT: Principles of construction, the main parameters and characteristics. *Instrumentation and Control Systems, 11*.

Donald, D. Dudenhoeffer etc CIMS: A framework for infrastructure interdependencies and analysis. *The2006Winter Simulation Conference (pp.478-485), Washington: on CD.*

Drimer, S. (2009). *Security for volatile FPGAs* (Technical Report N 763). Cambridge, UK: University of Cambridge Computer Laboratory.

DSTU. (1999). *Information technologies: Processes of software life cycle*. Kiev, Ukraine: State Committee of Ukraine on Standardization, Metrology and Certification.

DSTU-2850 (1994) Computer software – Metrics and methods for quality assessment. Ukrainian state standard.

Dubois, D., & Prade, H. (1980). *Fuzzy Sets and Systems: Theory and Application*. New York: Academic.

Duzhyi, V., Kharchenko, V., Starov, O., & Rusin, D. (2010). Research Sports Programming Services as Multi-version Projects. *Radioelectronic and Computer Systems*, *47*, 29–35.

EPRI TR1019181. (2009). *Guidelines on the use of field programmable gate arrays (FPGAs) in nuclear power plant I&C systems*. Electric Power Research Institute.

EPRI TR1022983. (2011). *Recommended approaches and design criteria for application of field programmable gate arrays in nuclear power plant I&C systems*. Electric Power Research Institute.

Everett, W., Keene, S., & Nikora, A. (1998). Applying Software Reliability Engineering in the 1990s. IEEE Transactions on Reliability 50th Anniversary Special Publication, 47 (3-SP), 372-378.

GAO-04-321. (2004). *Cybersecurity for critical infrastructure protection*. Washington, DC: U.S. General Accounting Office.

Gilchrist, W. (1998). Modeling failure modes and effects analysis. *International Journal of Quality & Reliability Management*, *10*(5), 16–23.

Glass, R. (2005). Simulation and Analysis of Cascading Failure in Critical Infrastructure. Working Together: R&D Partnerships in Homeland Security (pp. 45-56), Boston.

GND 306.7.02/2.041. (2000) Methodic of assessment of compliance of I & C systems to safety requirements. Kiev, Ukraine: State Nuclear Regulatory Committee.

GND. (2000). *Methods of assessment of compliance of I&C systems important to NPP: Safety with nuclear and radiation safety requirements*. Kiev, Ukraine: State Nuclear Regulatory Administration of Ukraine.

Goldrin, V. et al. (2001). NPP instrumentation and control systems safety standardization and assessment (3), principles of hardware life extension. *Nuclear and Radiation Safety*, *2*, 24–29.

Gorbenko, A., Kharchenko, V., & Romanovsky, A. (2009). Using Inherent Service Redundancy and Diversity to Ensure Web Services Dependability In Methods, Models and Tools for Fault Tolerance, M. Butler, C. Jones, A. Romanovsky, E. Troubitsyna (Eds.), pp. 324-341, LNCS 5454, Springer.

Gorelik, A., Eliseev, V., Kugil, A., et al. (2005). Conception of in-core reactor monitoring system modernization of Uktainian NPP. Nuclear and Radiation Safety, 2.

Gorochov, A. et al. (2004). *Explanation of neutron-physical and radiation parts in WWER design*. Moscow: Akademkniga.

GOST. (1991). GOST 29216. *Electromagnetic compatibility of technical means: Man-made noise from information technology equipment: Limits and test methods.*

GOST. (1992a). *Information technology: Types of testing of automated systems*. Moscow, Russia: Publishing House of Standards.

GOST. (1992b). *Information technology: Complex of standards on automated systems: Automated systems: Stages of creation*. Moscow, Russia: Publishing House of Standards.

GOST. (1998). *GOST 30546.1. Common requirements for seismic resistance of equipment, devices and other technical items and methods of their calculations*. GOST.

Grand, J. (2004). Practical secure hardware design for embedded systems. In *Proceedings of the 2004 Embedded Systems Conference*. San Francisco, CA: Academic Press.

Hashemian, H. (2006). *Maintenance of process instrumentation in nuclear power plants*. Berlin: Springer.

Hashemian, H. M. et al. (1998). *Advanced instrumentation and maintenance technologies for nuclear power plants (NUREG/CR-5501)*. Washington, DC: U.S. Nuclear Regulatory Commission.

Hashemian, H. M. (2005). *Sensor performance and reliability*. Research Triangle Park, NC: The Instrumentation, Systems and Automation Society.

Holmgren A., Molin S. (2006) Using Disturbance Data to Assess Vulnerability of Electric Power Delivery Systems. *Journal Infrastructure systems, American Society of Civil Engineers (ASCE), 12 (4), 243-251.*

Huang, H.-W., Wang, L.-H., Liao, B.-C., Chung, H.-H., & Jiin-Ming, L. (2011). Software safety analysis application of safety-related I&C systems in installation phase. *Progress in Nuclear Energy*, *6*(53), 736–741. doi:10.1016/j.pnucene.2011.04.002

Huffmire, T. et al. (2010). *Handbook of FPGA design security*. Berlin: Springer. doi:10.1007/978-90-481-9157-4

Hughes, P. J., & Johnson, G. L. (2000). Instrumentation and control systems important to safety: A new IAEA safety guide. International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000). Washington, DC: NPIC & HMIT.

IAEA. (1980). *50-SG-D3. Protection systems and related features in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1984). *50-SG-D8. Safety related instrumentation and control systems for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1988). *50-C-D. Code on the safety on nuclear power plants: Design*. Vienna, Austria: IAEA.

IAEA. (1997). *Safety problems of nuclear power plants with WWER-1000/320 reactors (IAEA EBP-WWER-05)*. Vienna, Austria: IAEA.

IAEA. (1998). *TECDOC-1016. Modernization of instrumentation and control in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1999). *Basic safety principles for nuclear power plants.75- INSAG-3, Rev. 1*. Vienna, Austria: IAEA.

IAEA. (1999). *INSAG-12. Basic safety principles for nuclear power plants (75-INSAG-3, Rev. 1)*. Vienna, Austria: IAEA.

IAEA. (1999). *Modern instrumentation and control for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1999). *Modern instrumentation and control for nuclear power plants: Guidebook (Technical reports series, Nº387)*. Vienna, Austria: IAEA.

IAEA. (1999a). *INSAG-12. Basic safety principles for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (1999b). *Modern instrumentation and control for nuclear power plants: A guidebook*. Vienna, Austria: IAEA.

IAEA. (1999c). *Verification and validation of software related to nuclear power plant instrumentation and control*. Vienna, Austria: IAEA.

IAEA. (2000a). *NS-R-1. Safety of nuclear power plants: Design: Safety requirements*. Vienna, Austria: IAEA.

IAEA. (2000b). *NS-G-1.1. Software for computer based systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2000c). *NS-R-2. Safety of nuclear power plants: Operation: Safety requirements*. Vienna, Austria: IAEA.

IAEA. (2002). *Instrumentation and control systems important to safety in nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2002b). *NS-G-2.3. Modifications to nuclear power plants: Safety guide*. Vienna, Austria: IAEA.

IAEA. (2006). *NS-G-1.3. Fundamental safety principles*. Vienna, Austria: IAEA.

IAEA. (2007). *Terminology used in nuclear safety and radiation protection: IAEA safety glossary*. Vienna, Austria: IAEA.

IAEA. (2009). *Safety assessment for facilities and activities: General safety requirements. IAEA safety standards series No. GSR Part 4*. Vienna, Austria: IAEA.

IAEA. (2010). *Governmental, legal and regulatory framework for safety: General safety requirements. IAEA safety standards series No. GSR Part 1*. Vienna, Austria: IAEA.

IAEA. (2011). *Computer security at nuclear facilities: Reference manual: Technical guidance*. Vienna, Austria: IAEA.

IAEA. (2011). *NP-T-3.12. Core knowledge on instrumentation and control systems in nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (2011a). *SSR-2/2. Safety of nuclear power plants: commissioning and operation: Specific safety requirements*. Vienna, Austria: IAEA.

IAEA. (2011a). *SSR-2/2. Safety of nuclear power plants: Commissioning and operation: Specific safety requirements*. Vienna, Austria: IAEA.

IAEA. (2012). *SSR-2/1. IAEA safety standards***:** *Safety of nuclear power plants: Design: Specific safety requirements*. Vienna, Austria: IAEA.

IAEA. (2012). *SSR-2/1. Safety of nuclear power plants: Design: Specific safety requirements*. Vienna, Austria: IAEA.

IAEA. (2013a). *DS-431. (Draft safety guide). Design of instrumentation and control systems for nuclear power plants*. Vienna, Austria: IAEA.

IAEA. (2013b). The statute of the IAEA. Retrieved from www.iaea.org/About/statute.html

IEC (2005a). IEC 62138. Nuclear power plants - Instrumentation and control important for safety -. Software aspects for computer-based systems performing category B or C functions.

IEC (2011). IEC 61513. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems.

IEC 60812 (2006). Analysis technique for system reliability – Procedure for Failure Mode and Effects Analysis (FMEA). International Electrotechnical Commission.

IEC 60880 (2006). Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. International Electrotechnical Commission.

IEC 60880. (2006). *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions.* IEC.

IEC 61025 (2006). Fault tree analysis. International Electrotechnical Commission.

IEC 61508 (2008). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. International Electrotechnical Commission.

IEC 61513. (2011). *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*. IEC.

IEC 62138. (2004). *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.* IEC.

IEC 62566. (2010). *Nuclear power plants – Instrumentation and control important to safety – Hardware language aspects for systems performing category A functions*. IEC.

IEC 62645. (2011). *Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems.* IEC.

IEC. (1980). IEC 60780. Nuclear power plants – Electrical equipment of the safety system – Qualification.

IEC. (1989). IEC 60980. Recommended practice for seismic qualification of electrical equipment for nuclear power generating stations.

IEC. (1989). IEC 60980. Recommended practices for seismic qualification of electrical equipment of the safety for nuclear generating stations.

IEC. (1996). IEC 60980. Recommended practice for seismic qualification of electrical equipment for nuclear power generating stations.

IEC. (1998). *Functional design criteria for safety parameter display system for nuclear power stations*. IEC.

IEC. (1998). IEC 60780. Nuclear power plants - Electrical equipment of the safety system – Qualification.

IEC. (2001). IEC 61838. Nuclear power plants – Instrumentation and control functions important for safety – Use of probabilistic safety assessment for the classification.

IEC. (2001a). IEC 61000-4-2. Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test.

IEC. (2001b). IEC 61000-4-3. Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity.

IEC. (2001c).: IEC 61000-4-4. Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques - Electrical fast transient / burst immunity test: Basic EMS publication.

IEC. (2001d). IEC 61000-4-8. Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test.

IEC. (2001e). IEC 61000-4-9. Electromagnetic compatibility (EMC) – Part 4-9: Testing and measurement techniques - Pulse magnetic field immunity test.

IEC. (2001f). IEC 61000-4-10. Electromagnetic compatibility (EMC) – Part 4-10: Testing and measurement techniques - Damped oscillatory magnetic field immunity.

IEC. (2001g). *IEC 61000-4-12:* Electromagnetic compatibility (EMC) – Part 4-12: Testing and measurement techniques - Oscillatory waves immunity test.

IEC. (2002a). *IEC 61000-4-14:* Electromagnetic compatibility (EMC) – Part 4-14: Testing and measurement techniques - Voltage fluctuation immunity test. IEC.

IEC. (2002b). IEC 61000-4-16. Electromagnetic compatibility (EMC) – Part 4-16: Testing and measurement techniques - Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz.

IEC. (2002c). IEC 61000-4-28. Electromagnetic compatibility (EMC) – Part 4-28: Testing and measurement techniques - Variation of power frequency, immunity test.

IEC. (2003). IEC 61511. Functional safety – Safety instrumental systems for the process industry sector.

IEC. (2004). IEC 61000-4-11. Electromagnetic compatibility (EMC) – Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests.

IEC. (2004a). IEC 60709. Nuclear power plants – Instrumentation and control systems important to safety – Separation.

IEC. (2004b). IEC 62138. Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.

IEC. (2005b). IEC 61000-4-5. Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques - Surge immunity test.

IEC. (2006). IEC 60880. *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.*

IEC. (2006a). IEC 61000-4-6. Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields.

IEC. (2006b). IEC 60880. Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.

IEC. (2007a). IEC 60050-394. *International electrotechnical vocabulary - Part 394: Nuclear instrumentation – Instruments, systems, equipment and detectors*.

IEC. (2007a). IEC 62342. Nuclear power plants – Instrumentation and control systems important to safety – Management of aging.

IEC. (2007b). IEC 60987. *Nuclear power plants – Instrumentation and control important to safety –Hardware design requirements for computer-based systems.*

IEC. (2007b). *IEC 62340. Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure*. CCF.

IEC. (2007c). IEC 60987. Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems.

IEC. (2008). *Functional safety of electrical/electronic/programmable electronic safety/related systems*. IEC.

IEC. (2009). IEC 61226. Nuclear power plants -Instrumentation and control systems important to safety – Classification.

IEC. (2009a). IEC 60964. Nuclear power plants – Control rooms – Design.

IEC. (2009c). IEC 61226. Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category a functions.

IEC. (2011). IEC 61513. *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*.

IEC. (2011). *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*. IEC.

IEC/IEEE. (2011). IEC/IEEE 62582. Nuclear power plants – Instrumentation and control important to safety – Electrical equipment condition monitoring methods – Part 1: General: Part 2: Indenter modulus: Part 4: Oxidation induction techniques.

IEEE 610.12 (1990). Standard Glossary of Software Engineering Terminology. Institute of Electrical and Electronics Engineers.

IEEE 982.2 (1988). Standard Guide of Measures to Produce Reliable Software. Institute of Electrical and Electronics Engineers.

IEEE. (1978). IEEE 338. *IEEE standard criteria for the periodic surveillance testing of nuclear power generating station safety systems*.

IEEE. (2010). IEEE std. 497.2010. IEEE standard criteria for accident monitoring instrumentation for nuclear power generating stations.

ISO. (2000). ISO 9001. *Quality management systems - Requirements*.

ISO. (2000). ISO 9001. Quality management systems – Requirements.

ISO. IEC 9126-1 (1999). Information technology. Software product quality – Part 1: Quality model. International Organization for Standardization.

ISO/IEC 15408. (2009). *Information technology – Security techniques – Evaluation criteria for IT security*. ISO/IEC.

ISO/IEC 17799. (2005). *Information technology – Security techniques – Code of practice for information security management*. ISO/IEC.

ISO/IEC 27000. (2009). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. ISO/IEC.

ISO/IEC 27001. (2005). *Information technology – Security techniques – Information security management systems – Requirements.* ISO/IEC.

ISO/IEC 27002. (2005). *Information technology – Security techniques – Code of practice for information security management.* ISO/IEC.

ISO/IEC 27003. (2010). *Information technology – Security techniques – Information security management system implementation guidance.* ISO/IEC.

ISO/IEC 27004. (2009). *Information technology – Security techniques – Information security management – Measurement.* ISO/IEC.

ISO/IEC 27005. (2011). *Information technology – Security techniques – Information security risk management.* ISO/IEC.

ISO/IEC 27006. (2011). *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.* ISO/IEC.

ISO/IEC 27007. (2011). *Information technology – Security techniques – Guidelines for information security management systems auditing.* ISO/IEC.

ISO/IEC 27008. (2011). *Information technology – Security techniques – Guidelines for auditors on information security management systems controls.* ISO/IEC.

ISO/IEC TR 9126 (2000). Information technology. Software product quality – Part 2: External metrics; Part 3: Internal metrics; Part 4: Quality in use metrics. International Organization for Standardization.

ISO/IEC. (2008). *Systems and software engineering – Software life cycle processes*. ISO/IEC.

Johnson, G. (2002). Comparison of IEC and IEEE standards for computer-based control systems important to safety. In Proceedings of CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems. AEN/NEA.

Johnson, B., & Christensen, L. (2008). *Educational research: Quantitative, qualitative, and mixed approaches*. Thousand Oaks, CA: Sage Publications. doi:10.1093/swr/32.1.3

Jonson, G. (2010). The INSAG Defense in Depth Concept and D-in-D&D in I&C. Paper presented at the meeting of the *7th ANS Topical Meeting on NPIC-HMIT, Las Vegas, USA*.

Kaijser, A. (1984). *The Swedish Infrastructure – Historical Development and Future Challenges*. Stockholm: Carlsson.

Karry, R., et al. (2010, October). Trustworthy hardware: Identifying and classifying hardware trojans. *Computer Magazine*, 39-46. Christiansen, B. (2006). *Active FPGA security through decoy circuits*. (MS Thesis). Air Force Institute of Technology.

Kersken, M. (2001). Qualification of pre-developed software for safety-critical I&C application in NPP's. Paper presented at CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, Hluboka-nad-Vltavou, Czech Republic.

Kharchenko, V. (1999). Multi-version Systems: Models, Reliability, Design Technologies. *The 10th ESREL Conference: Vol.1, pp. 73-77.* Munich, Germany.

Kharchenko, V. S. (Ed.). (2012). CASE-assessment of critical software systems. Quality. Reliability. Safety. Kharkiv, Ukraine: National Aerospace University KhAI.

Kharchenko, V. S., & Vilkomir, S. A. (2000). The Formalized Models of Software Verification Assessment. Paper presented at 5th International Conference Probabilistic Safety Assessment and Management, Osaka, Japan.

Kharchenko, V. Siora O., Sklyar V. (2011). Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring, Nuclear Power - Control, Reliability and Human Factors, Dr. Pavel Tsvetkov (Ed.), InTech, from: http://www.intechopen.com/books/nuclear-power-control-reliability-and-human-factors/multi-version-fpga- based-nuclear-power-plant-i-c-systems-evolution-of-safety-ensuring.

Kharchenko, V., & Sklyar, V. (2008). *FPGA-based NPP instrumentation and control systems: Development and safety assessment*. Kharkov, Ukraine: Zhukovsky National Aerospace University KhAI.

Kharchenko, V., Duzhyi, V., Sklyar, V., & Volkoviy, A. (2012). Safety Assessment of Multi-version FPGA-based NPP I&C Systems: Theoretical and Practical Issues. Paper presented at the meeting of the *5th International Workshop on the Applications of FPGA in Nuclear Power Plants, Beijing*.

Kharchenko, V., et al. (2001). Methodology of NPP I&C system algorithms and software veri-fication expert analysis. In *Proceedings of Workshop on Licensing and Operating Experience of Computer-Based I&C Systems*. Hluboka-nad-Vltavou, Czech Republic: Academic Press.

Kharchenko, V., et al. (2004). *Methods of modeling and assessment of software quality and dependability*. Kharkov, Ukraine: Zhukovsky National Aerospace University KhAI.

Kharchenko, V., et al. (2004). The technique and the experience of expertise of software for NPP: Instrumentation and control systems. In *Proceeding by 7th International Conference on Probabilistic Safety Assessment and Management and European Safety and Reliability Conference*. Berlin, Germany: Academic Press.

Kharchenko, V., et al. (2011). Critical infrastructures safety: Mathematical and engineering methods of analysis and assurance. Department of Education and Science of Ukraine, National Aerospace University named after N. Zhukovsky KhAI. IEC 61508: Ed. 2. (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems. (IEEE 982.2, 1988)

Kharchenko, V., et al. (2012a). Cyber security of FPGA-based NPP I&C systems: Challenges and solutions. In *Proceeding of the 8th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies* (NPIC & HMIT 2012). San Diego, CA: NPIC & HMIT.

Kharchenko, V., et al. (2012d). Cyber security lifecycle and assessment technique for FPGA-based I&C systems. In *Proceeding of IEEE East-West Design & Test Symposium* (EWDTS'2012). Kharkov, Ukraine: IEER.

Kharchenko, V., Siora, A., & Bakhmach, E. (2008). Diversity-scalable decisions for FPGA-based safety-critical I&C systems: from Theory to Implementation. Paper presented at the meeting of the *6th Conference NPIC&HMIT, Knoxville, USA*.

Kharchenko, V., Siora, A., Sklyar, V., & Volkoviy, A. (2012). Defence-in-Depth and Diversity Analysis of FPGA-based NPP I&C Systems: Conception, Technique and Tool. Paper presented at the meeting of the *ICONE20, Anaheim, USA*.

Kharchenko, V., Siora, A., Sklyar, V., Volkoviy, V., & Bezsaliy, V. (2010). Multi-Diversity Versus Common Cause Failures: FPGA-Based Multi-Version NPP I&C Systems. Paper presented at the meeting of the *7th Conference NPIC&HMIT, Las-Vegas, USA*.

Kharchenko, V., Sklyar, V., & Volkoviy, A. (2007). Multi-Version Information Technologies and Development of Dependable Systems out of Undependable Components. Paper presented at the meeting of the *International Conference on Dependability of Computer Systems,Szklarsla Poreba, Poland*.

Kharchenko, V., Sklyar, V., Siora, A., & Tokarev, V. (2008). Scalable Diversity-oriented Decisions and Technologies for Dependable SoPC-based Safety-Critical Computer Systems and Infrastructures. Paper presented at the meeting of the *IEEE International Conference on Dependability of Computer Systems, Szklarska Poreba, Poland*.

Kharchenko, V., Yastrebenetsky, M., & Sklyar, V. (2004). Diversity Assessment of Nuclear Power Plants Instrumentation and Control Systems, *The 7th International Conference on PSAM and ESREL Conference, Volume 3, pp.1351-1356*. Berlin, Germany.

Kharchenko, V. et al. (2002). NPP instrumentation and control systems safety standardization and assessment (7), regulatory requirements on software. *Nuclear and Radiation Safety*, *1*, 18–33.

Kharchenko, V. et al. (2012b). GAP- and HTT-based analysis of safety-critical systems. *Radioelectronic and Computer Systems*, *7*(59), 198–204.

Kharchenko, V. et al. (2012c). Gap-and-IMECA-based assessment of I&C systems cyber security. *Advances in Intelligent and soft*. *Computing*, *170*, 149–164.

Kharchenko, V. S., & Sklyar, V. V. (Eds.). (2008). *FPGA-based NPP instrumentation and control systems: Development and safety assessment. Research and Production Corporation Radiy, National Aerospace University named after N.E. Zhukovsky KhAI*. State Scientific Technical Center on Nuclear and Radiation Safety.

Kharchenko, V., & Sklyar, V. (Eds.). (2008). *FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment, RPC Radiy, National Aerospace University "KhAI"*. State Scientific and Technical Center for Nuclear and Radiation Safety.

Kharchenko, V., & Sklyar, V. (Eds.). (2008). *FPGA-based NPP: Instrumentation and control systems: Development and safety assessment. National Aerospace University KhAI*. State Scientific and Technical Centre for Nuclear and Radiation Safety.

Khvastunov, R. et al. (1981). *Expert assessments and their application in power engineering*. Moscow, Russia: Energoizdat.

Klevtsov, A., & Yastrebenetsky, M. (2007c). Perspectives of developing and using of knowledge base at NPP's I&C for expert activity support. In *Proceedings of International Conference on Knowledge Management in Nuclear Facilities: Book of Extended Synopsis* (pp. 119-120). Vienna, Austria: IAEA.

Klevtsov, A. (2007a). The knowledge base for safety assessment of NPP's instrumentation and control systems. *Radio Electronic and Computer Systems*, *7*, 114–120.

Klevtsov, A. (2007b). Creating and using of knowledge base for support of expert activity. *Nuclear and Radiation Safety*, *1*, 86–97.

Klevtsov, A. (2008a). Development of automated system for support of expert activity during safety assessment of instrumentation and control systems. In *Modeling and analysis of safety and risk in complex systems: Proceedings of international scientific school MASR-2008* (pp. 420–425). Saint Petersburg, Russia: Saint-Petersburg State University of Aerospace Instrumentation.

Klevtsov, A. (2008b). The model for safety assessment of NPP's instrumentation and control systems under nuclear and radiation safety expert reviewing. *Radio Electronic and Computer Systems*, *7*, 53–58.

Kolesov, S., et al. (2000). Safety parameters display system (SPDS) for Ukrainian NPP with WWER-1000 reactor type. In *Proceedings of International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies* (NPIC&HMIT 2000). Washington, DC: NPIC & HMIT.

Konorev, B. et al. (2007). Target technology of cost-effective assessment of reliability and functional safety of critical software. *Radio Electronic and Computer Systems*, *6*, 162–170.

Konorev, B. et al. (2010). Independent verification and prediction of hidden defects of software of critical systems: Complex of static analysis tools. In *Problems of safety assurance of NPP instrumentation and control systems: Collected articles* (pp. 152–156). Odessa, Ukraine: Astroprint.

KTA. (1985). *KTA 3501. Reactor protection system and monitoring equipment of the safety system*. Cologne, Germany: GRS.

Lahtinen, J., Valkonen, J., Bjorkman, K., Frits, J., & Niemela, I. (2010). Model checking methodology for supporting safety critical software development and verification. Paper presented at ESREL 2010 Annual Conference, Rhodes, Greece.

Larichev, O. (2008). *Theory and methods of decisions-making*. Moscow, Russia: Logos.

Law of Ukraine. (1995). *On nuclear energy use and radiation safety*. Kiev, Ukraine: Verkhovna Rada of Ukraine.

Law of Ukraine. (2000). *On authorizing activity in nuclear energy use*. Kiev, Ukraine: Verkhovna Rada of Ukraine.

Lawrence, S., Hatton, L., & Howell, C. (2002). *Solid Software*. Prentice Hall.

Leech, N., & Onwuegbuzie, A. (2008). Qualitative data analysis: A compendium of techniques for school psychology research and beyond. *School Psychology Quarterly*, *23*, 587–604. doi:10.1037/1045-3830.23.4.587

Lindner, A., & Wach, D. (2008). Experiences gained from independent assessment in licensing of advanced I&C systems in nuclear power plants. *Nuclear Technology*, *143*, 197–207.

Linstone, H. (1984). Multiple Perspectives for Decision-Making: Bridging the Gap Between Analysis and Action, Holland, Amsterdam.

Lyu, M. R. (1996). *Handbook of software reliability engineering*. New York: McGraw-Hill Company.

Makhutov, N. et al. (2009). *Risk analysis and safety improving of water-water power reactors*. Moscow: Nauka.

McCabe, T. A. (1976). Complexity measure. *IEEE Transactions on Software Engineering*, *4*(2), 308–320. doi:10.1109/TSE.1976.233837

Melnyk, A., et al. (2007). Automatic generation of ASICS. In *Proceedings of NASA/ESA Conference on Adaptive Hardware and Systems*. Edinburgh, UK: NASA/ESA.

Mendel, J. M. (2002). An architecture of making judgment using computing with words. *International Journal of Applied Mathematics and Computer Science*, *12*(3), 325–335.

Miedl, H. (2010). Qualification of field equipment with software for systems important to safety. In *Problems of safety assurance of NPP instrumentation and control systems: Collected articles* (pp. 133–166). Odessa, Ukraine: Astroprint.

Moskalenko, N., & Sokolnokova, T. (2010). Smart Grid – German and Russian Perspectives in Comparison. *International Conference on Modern Electric Power Systems 2010, (pp.23-30), Wroclaw, Poland*

NAPB. (2002). *NAPB 03.005. Fire protection: Firefighting norms development of nuclear power plants with pressured water reactors*. Kiev, Ukraine: Ministry of Fuel and Energy.

NARB. (2000). *Fire protection: Firefighting norms development of nuclear power plants with pressured water reactors*. Kiev, Ukraine: Ministry of Fuel and Energy.

Naser. (Ed.). (2009). Guidelines on the use of field programmable gate arrays (FPGAs) in nuclear power plant I&C systems. Palo Alto, CA: EPRI.

NEI 08-09. (2010). *Cyber security plan for nuclear power reactors*. Nuclear Energy Institute.

Nikituk, V. et al. (2004). *WWER control rod drives for nuclear power plants*. Moscow: Akademkniga.

Nikituk, V. et al. (2004). *WWER reactors SUZ drives for nuclear power plants*. Moscow: Akademkniga.

NIST SP 800-30. (2002). *Risk management guide for information technology systems*. Washington, DC: National Institute of Standards and Technology.

NIST SP 800-53. (2009). *Recommended security controls for federal information systems and organizations*. Washington, DC: National Institute of Standards and Technology.

Nosovsky, A., Vasilchenko, V., & Pavlenko, A. et al. (2006). *Safety of nuclear power plants: Introduction into safety of nuclear technology*. Kiev, Ukraine: Technika.

NP. (1999). NP 306.5.02/3.017. Quality assurance program requirements at all stages life-cycle of the nuclear power plant. Kiev, Ukraine: State Committee for nuclear regulation.

NP. (2000). *NP 306.5.02/3.035. Requirements for nuclear and radiation safety information and control systems important to safety of nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2000). *Nuclear and radiation safety requirements to instrumentation and control systems important to nuclear power plants safety*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2000a). *General regulations of nuclear power plant safety assurance*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2000b). *Requirements for nuclear and radiation safety of information and control systems important to the safety of nuclear power plants*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2003). *Requirements to order and contents to life extension of instruments which included to safety important systems*. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. (2003a). *NP 306.5.02/2.068. Requirements for the order and scope of work to extend the term operation activity of information and control systems, important to safety of nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2003b). *NP 306.5.02/3.076. Requirements for the organization and order of commissioning power plant*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2005). *NP 306.2.106. Requirements for the modification of the nuclear installations and their safety evaluation order*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2005a). *Procedure for state review of nuclear and radiation safety*. Kiev, Ukraine: State Nuclear Regulatory Administration of Ukraine.

NP. (2005b). *Requirements for modification of nuclear plants and an order of their safety assessment*. Kiev, Ukraine: State Nuclear Regulatory Administration of Ukraine.

NP. (2008a). *NP 306.2.141. General provisions on the safety of nuclear power plants*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. (2008b). *NP 306.2.145. Nuclear safety regulations the reactors nuclear power plants with pressurized water reactors*. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. NP 306.2.145. (2008b). Nuclear safety regulations the reactors nuclear power plants with pressurized water reactors. Kiev, Ukraine: State Nuclear Regulatory Committee.

NP. NP 306.5.02/3.035. (2000). Nuclear and radiation safety requirements to instrumentation and control systems important to safety to nuclear power plants. Kiev, Ukraine: State Committee for Nuclear Regulation.

NP. NP-001-97. (1997). General provisions on the safety of nuclear power plants. Moscow, Russia: Russian Federal Supervision on Nuclear and Radiation Safety.

NS-G-1. 1 (2000). Software for computer based systems important to safety in nuclear power plants. Vienna, Austria: IAEA.

NUREG. (2002). NUREG-0800. *US nuclear regulatory commission: Standard review plan: Section 7.0: Instrumentation and control - Overview of review process*.

NUREG/CR-6003. (1994). *Method for performing diversity and defense-in-depth analyses of reactor protection systems*. Washington, DC: United States Nuclear Regulatory Commission.

NUREG/CR-7006. (2010). *Review guidelines for field-programmable gate arrays in nuclear power plant safety systems*. Washington, DC: U.S. Nuclear Regulatory Commission.

NUREG/CR-7007. (2009). *Diversity strategies for NPP I&Cs*. Washington, DC: United States Nuclear Regulatory Commission.

Ostreikovsky, V., & Shviraev, Y. (2008). *Safety of nuclear power plants: Probability analysis*. Moscow: Fizmatlit.

Plutinsky, V., & Pogorelov, B. (1983). *Automatic control and protection of NPP. heat-energetic installation*. Moscow: Energy.

PNAE. (1987). *PNAE G-5-006. Rules of design earthquake-resistant nuclear power plants*. Moscow: Gosatomenergonadzor.

Pressman, R. S. (1997). *Software Engineering: A Practioner's Approach*. McGraw-Hill Company.

Prokhorova, Y., Kharchenko, V., Ostroumov, B., Ostroumov, S., & Sidorenko, N. (2008). Dependable SoPC-Based On-board Ice Protection System: from Research Project to Implementation. Paper presented at the meeting of the *IEEE International Conference on Dependability of Computer Systems, Szklarska Poreba, Poland.*

Pullum, L. (2001). *Software fault tolerance techniques and implementation*. Artech House Computing Library.

Ravi, S. et al. (2004). Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems*, *3*(3), 461–491. doi:10.1145/1015047.1015049

Rezepov, V. et al. (2004). *VVER-1000 reactors for nuclear power plants*. Moscow: Akademkniga.

RG 5.71. (2010). *Cyber security programs for nuclear facilities.* Washington, DC: U.S. Nuclear Regulatory Commission.

Rosenberg, M., & Bobryakov, S. (2003). *Elsevier's dictionary on nuclear engineering*. London: Elsevier Science.

Rozen, Y. (2007). Electromagnetic compatibility of instrumentation and control systems components (1), rules for regulations and estimation. Nuclear and Radiation Safety, 2.

Rozen, Y. (2008). Electromagnetic compatibility of instrumentation and control systems components (2), Устойчивость к электромагнитным помехам. Nuclear and Radiation Safety, 4.

Sadeghi, A.-R. et al. (2011). *Towards hardware-intrinsic security: Foundations and practice*. Berlin: Springer.

Samoilov, O. et al. (1989). *Safety of nuclear energetical installation*. Moscow: Energoizdat.

Scott, J., & Lawrence, J. (1994). *Testing existing software for safety related applications*. Lawrence Livermore National Laboratory.

Sergienko, V. et al. (2008). Calibration of invariants measurements methods of critical software: Profile of injecting test faults. *Radio Electronic and Computer Systems*, *5*, 161–167.

Siora, A., Sklyar, V., Rozen, Yu., Vinogradskaya, S., & Yastrebenetsky, M. (2009). Licensing Principles of FPGA-Based NPP I&C Systems. Paper presented at the meeting of the *17th International Conference on Nuclear Engineering, Brussels, Belgium.*

Siora, A., Krasnobaev, V., & Kharchenko, V. (2009). *Fault-Tolerance Systems with Version-Information Redundancy*. Ukraine: Ministry of Education and Science of Ukraine, National Aerospace University KhAI.

Sklyar, V., & Kharchenko, V. (2006). Safety features and assessment of software of NPP instrumentation and control systems. *Nuclear Measuring-Information Technologies*, *1*, 3–18.

Smith, J., & Simpson, K. (2001). *Functional safety: A straightforward guide to IEC 61508 and related standards*. Oxford, UK: Butterworth Heinemann.

Sommerville, J. (2011). *Software engineering* (9th ed.). Reading, MA: Addison-Wesley.

Storey, N. (1996). *Safety-critical computer systems*. Reading, MA: Addison Wesley Longman.

Tam, S. (2003). *Error detection and correction in virtex-II pro devices*. Application Note: Virtex-II Pro Family. XAPP645 (v1.1).

Tarasyuk, O., Gorbenko, A., Kharchenko, V., Ruban, V., & Zasukha, S. (2011). Safety of Rocket-Space Engineering and Reliability of Computer Systems: 2000-2009 Years. *Radio-Electronic and Computer Systems*, *11*, 23–45.

Tehranipoor, M., et al. (2010). A survey of hardware trojan taxonomy and detection. In *Proceedings of IEEE Design & Test of Computers*. IEEE.

Tokarenko, V. (2000). System of safety analysis of atomic technologies SABAT. *Issues of Atomic Science and Technique*, *3*, 45–70.

USNRC. (1981). *Functional criteria for emergency response facilities*. Washington, DC: U.S. Nuclear Regulatory Commission.

USNRC. (2010). Standard review plan for the review of safety analysis reports for nuclear power plants: LWR Ed. section 7.0: Instrumentation and control - Overview of review process (rev. 6). Washington, DC: US Nuclear Regulatory Commission.

Vilkomir, S. (2009). Statistical testing for NPP I&C system reliability evaluation. Paper presented at the meeting of the *6th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, Knoxville, USA.*

Vilkomir, S. A., & Kharchenko, V. S. (1999). Methodology of the review of software for safety important systems. In G. I. Schueller, P. Kafka (Eds). Safety and Reliability. Proceedings of ESREL'99 - The Tenth European Conference on Safety and Reliability (pp. 593-596). Munich-Garching, Germany.

Vilkomir, S., & Kharchenko, V. (2000). An "asymmetric" approach to the assessment of safety-critical software during certification and licensing. Paper presented at ESCOM-SCOPE 2000 Conference, Munich, Germany.

Vilkomir, S., Swain, T., & Poore, J. (2009). Software Input Space Modeling with Constraints among Parameters. Paper presented at the meeting of the *33rd Annual IEEE International Computer Software and Applications Conference COMPSAC, Seattle.*

Yastrebenetsky, M., & Vasilchenko, V. (2001f). Expert evaluation in NPP safety important systems licensing process. In *Proceedings of the 9-th International Conference on Nuclear Engineering*. Nice, France: Academic Press.

Yastrebenetsky, M., et al. (2012). Strategy of NPP I&C systems modernization in Ukraine. In *Proceeding of 8th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology* (pp. 593-599). San Diego, CA: American Nuclear Society.

Yastrebenetsky, M., Rozen, Y., et al. (2010). Ukrainian NPP I&C standard base: Elaboration and application. In Proceedings of Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010. Las Vegas, NV: American Nuclear Society.

Yastrebenetsky, M., Rozen, Y., Gromov, G., et al. (2011). *Requirements to instrumentation and control systems according results of analysis of Fukushima-1 accident. Nuclear and Radiation Safety, 4*.

Yastrebenetsky, M., Rozen, Y., Klevtsov, A., et al. (2012). Fukushima accident lessons for I&C systems. Paper presented at the 8th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies (NPIC & HMIT). San Diego, CA.

Yastrebenetsky, M., Rozen, Y., Siora, A., et al. (2010). Ukrainian NPP I&C regulatory framework: Elaboration and application. Paper presented at the International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies-7. Las Vegas, NV.

Yastrebenetsky, M. et al. (2001a). NPP instrumentation and control systems safety standardization and assessment (1), objects, aims, tasks. *Nuclear and Radiation Safety*, *1*, 20–28.

Yastrebenetsky, M. et al. (2001b). NPP instrumentation and control systems safety standardization and assessment (2), principles of standardization. *Nuclear and Radiation Safety*, *2*, 16–23.

Yastrebenetsky, M. et al. (2001c). NPP instrumentation and control systems safety standardization and assessment (4), principles of assessment. *Nuclear and Radiation Safety*, *3*, 17–30.

Yastrebenetsky, M. et al. (2001d). NPP instrumentation and control systems safety standardization and assessment (5), regulatory requirements on systems. *Nuclear and Radiation Safety*, *3*, 31–37.

Yastrebenetsky, M. et al. (2001e). NPP instrumentation and control systems safety standardization and assessment (6), regulatory requirements on hardware. *Nuclear and Radiation Safety*, *4*, 11–25.

Yastrebenetsky, M. et al. (2002a). NPP instrumentation and control systems safety standardization and assessment (8), automatic control algorithms assessment. *Nuclear and Radiation Safety*, *2*, 23–36.

Yastrebenetsky, M. et al. (2002b). NPP instrumentation and control systems safety standardization and assessment (9), procedures of assessment and their information support. *Nuclear and Radiation Safety*, *3*, 40–57.

Yastrebenetsky, M. et al. (2004). *Safety of nuclear power plants: Instrumentation and control systems*. Kiev, Ukraine: Technique.

Yastrebenetsky, M., Vasilchenko, V., & Vinogradska, S. et al. (2004). *Nuclear power plants safety: Instrumentation and control systems*. Kiev: Technika.

Zadeh, L. (2009). From computing with numbers to computing with words-from manipulation of measurements to manipulation of perceptions. *IEEE Trans.Circ. Syst, Fund. TheoryApplic.*, *4*(1), 105–119.

Zadeh, L., & Kacprzyk, J. (1999). Computing with Words in Information/Intelligent Systems – Part 1:Foundation; Part 2: Applications. *Heidelberg, Germany*. *Physica-Verlag*, *1*, 187–201.

About the Contributors

Mikhail Yastrebenetsky, PhD, Doctor of technical sciences, Professor, Honor scientist of Ukraine. Until 1992 – Head of Department “Reliability of Automated Control Systems” of the Central Scientific Research Institute of Complex Automation. Since 1993 – head of the Department “NPP Control and Information Systems Safety Analysis” of State Scientific and Technical Centre of Nuclear and Radiation Safety Professor of the Department “Systems Analysis and Control” of the Kharkov National Technical University. Author of 12 monographs, 290 articles, 35 international and national standards and regulations. Organizer and Chairman of 1-5 International Conferences “NPP I&C systems: safety aspects”. Expert of IEC.

Vyacheslav Kharchenko, PhD (1981), Doctor of technical sciences (1995), Professor (1991), Honor inventor of Ukraine (1990). Head of the Department of aerospace control systems, Kharkiv Military University (1992). Head of the Department of computer systems and networks, National Aerospace University KhAI (2001-present), Director of the Center for safety infrastructure-oriented research and analysis, RPC Radiy (2006-present). General chair of the DESSERT Conferences (2006-2013), SERENE Workshop (2013). Invited lecturer of a lot of international conferences and universities. The author of 32 monographs and textbooks, more than 700 inventions, 200 articles (70 articles published in English). Supervisor of 40 PhD and DrS-students.

***

Anton Andrashov is head of international projects division at RPC Radiy. He received his B.S. (2005) and M.S. (2007) with honor degrees in Computer Engineering from National Aerospace University KhAI. Lecturer assistant at the Department of computer systems and networks, KhAI (2007- 2011). Senior researcher at the Centre for safety infrastructure-oriented research and analysis (2008-2011). Currently involved in implementation of several international projects including SIL 3 certification of FPGA-based safety platform for NPP I&C systems. The author of 3 monographs and textbooks, more than 40 articles, including articles published in the Japan, Germany, USA, and other countries.

Eugene Babeshko, MS in Computer engineering (2007). Head of division at software department, Khartep Ltd. (2010), Senior lecturer at the Department of computer systems and networks, National Aerospace University KhAI (2007-present), Researcher at the Center for safety infrastructure-oriented research and analysis, RPC Radiy (2010-present). Certified specialist on industrial controllers (2004, 2006, 2011), functional safety assessment (2010). The author of more than 30 papers in the fields of industrial controllers, I&C systems, reliability and safety assessment.

Eugene Brezhnev, PhD (2000). Senior researcher, Kharkiv Military University (2010), Doctoral of technical science student (2010-2013), associate professor at the Department of computer system and network, National Aerospace University KhAI (2012-present). Senior researcher at the Center for safety infrastructure-oriented research and analysis, RPC Radiy (2011-present). The author of 2 monographies, 78 articles, including 12 articles published in the Great Britain, USA, and other countries.

Vladislav Goldrin, PhD. Until 1992 – head of a laboratory at Central Scientific Research Institute of Complex Automation. Since 1993 – leading researcher of State Scientific and Technical Centre for Nuclear and Radiation Safety. Author of 32 articles and 6 intergovernmental standards and normative documents on nuclear safety.

Grygoriy Gromov, PhD. Since 1988 to 1992 – design engineer in the Kiev Division of the Atomenergoproject Institute. Since 1992 worked in State Scientific and Technical Centre for Nuclear and Radiation Safety (SSTC NRS) – Technical Support Organization of State Nuclear Regulatory Inspectorate of Ukraine. Since 2009 – Director of SSTC NRS. Performed R&D on NPP nuclear and radiation safety, developed certain part of NPP Safety Analysis Reports for nuclear industry in Ukraine. Author of more than 20 articles in scientific and technical journals, IAEA documents. Vice-President of European Technical Safety Organization Network. (ETSON).

Vladislav Inyushev, PhD. Since 1993 worked in the State Scientific and Technical Center for Nuclear and Radiation Safety (SSTC NRS) – Technical Support Organization of State Nuclear Regulatory Inspectorate of Ukraine. Since 2002 – Deputy director of SSTC NRS on safety assessment. Realized scientific and methodical leadership on expert analysis of nuclear and radiation safety of different types of NPP systems, including NPP instrumentation and control systems. Author of more than 30 articles in scientific and technical journals, IAEA documents.

Alexander Klevtsov, PhD (2010). Since 1999 worked in Kharkov subsidiary of the State Scientific and Technical Centre for Nuclear and Radiation Safety (SSTC NRS). Since 2009 – Head of “Laboratory of safety analysis of information systems” of SSTC NRS. Carry out the expert analysis of nuclear and radiation safety and reliability assessment of NPP instrumentation and control systems. Author of more than 25 articles in scientific-technical journals and 5 books about programming languages, took part in elaboration of 3 national standards.

Andriy Kovalenko, PhD (2008), Associate Professor (2012). Assistant professor (2009), associate professor at the Department of Computer Engineering and Control, Kharkiv National University of Radioelectronics (2010-present). Senior researcher at the Center for safety infrastructure-oriented research and analysis, RPC Radiy (2009-present). The author of more than 70 papers (including conference proceedings).

Yuri Rozen was, until 1995, head of a department, deputy director for scientific work, chief designer of the Scientific and Manufacturing Enterprise on Automated Control Systems. Since 2001 – head of a laboratory of State Scientific and Technical Centre for Nuclear and Radiation Safety. Twice was a winner of a prize of the USSR Council of Ministers. Held the rank “best inventor of instrument construction”. Author of 3 books, 82 articles, 26 inventions, 48 intergovernmental and national standards and normative documents on nuclear safety.

Alexander Siora, PhD (2005). General director of RPC Radiy (1998-present). Associated professor at the Department of computer systems and networks, National Aerospace University KhAI (2006-2012). He received a few honor awards for successes related to research, development and implementation of NPP I&C systems, including medal of Ukrainian National Academy of Science (2010). The author of 5 monographs and textbooks, more than 80 articles and reports, including 20 articles published in English.

Vladimir Sklyar, PhD (2001), Doctor of technical sciences (2012). Senior researcher at the State Scientific Technical Centre for Nuclear and Radiation Safety (2002), Technical Director of RPC Radiy (2011-present), Associated Professor (2002) and Professor (2012-present) at the Department of computer systems and networks, National Aerospace University KhAI. The author of 10 monographs and textbooks, more than 100 articles, including 30 articles published in English.

Svetlana Vinogradska, PhD. Until 1992 – senior researcher of Central Scientific Research Institute of Complex Automation. Since 1993 – head of a laboratory of State Scientific and Technical Centre for Nuclear and Radiation Safety. Author of 2 books, 54 articles and 5 normative documents on nuclear safety.

Andriy Volkoviy, PhD (2006), associated professor (2012). More than 10 years taught programming languages and software engineering technologies at Department of computer systems and networks, National Aerospace University KhAI (2000-2012). Along with teaching participated in projects for Ukrainian regulation and certification authorities in the area of critical software-based I&C systems. Senior researcher of the Center for safety infrastructure-oriented research and analysis, RPC Radiy (2006-2012). Senior research and development engineer of Samsung Electronics Ukraine Research Center (2012-present). The author of 10 textbooks, more than 50 articles and reports.

Index