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**


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