THE IAEA SAFETY PRINCIPLES APPLIED TO NPP INSTRUMENTATION AND CONTROL

Björn Wahlström
Systems Analysis Laboratory, Aalto University
Otakaari 1F, FI-02150 Espoo, Finland
bjorn.wahlstrom@aalto.fi

Alex Duchac
International Atomic Energy Agency
P.O. Box 100, Wagramer Strasse 5, A-1400 Vienna, Austria
A.Duchac@iaea.org

ABSTRACT

The International Atomic Energy Agency (IAEA) has produced many important documents that govern nuclear power plant (NPP) design. The documents have in several countries been applied in national legislation on nuclear facilities. The documents are sometimes due to their sheer volume inaccessible, but they have a logical structure that helps users to orient among the documents. Especially if basic safety principles are lifted up together with their subordinate principles, a structure that is easy to understand starts to emerge. The paper goes through IAEA safety standards and supporting documents applicable to instrumentation and control (I&C) in system design as well as operation and maintenance and shows how these documents are interconnected.

Key Words: IAEA documents, safety principles, safety assessments, design guides.

1 INTRODUCTION

The International Atomic Energy Agency (IAEA) has an important role in the nuclear area, both as a promoter of nuclear power for peaceful use and as an agent to guard against the proliferation of nuclear weapons. The organisation was established in 1957 as a response to a speech at the General Assembly of the United Nations on 8 December 1953 by Dwight D. Eisenhower, the President of the United States of America [1]. IAEA soon adopted a role to support the international exchange of information on peaceful use of nuclear power among member countries.

In order to support the development and implementation of instrumentation and control (I&C) systems important to safety, the IAEA established an International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI) in 1970. Since then, the group has become an important forum for information exchange between I&C experts all over the world. The group has arranged several workshops, conferences and coordinated research programmes from which material can be downloaded from the IAEA web-pages. Today the I&C topic is organised in the Instrumentation and Control Technologies group of the Nuclear Power Engineering department in IAEA (http://www.iaea.org/NuclearPower/IandC/).

This paper highlights important achievements of the working group that have considerable impact on the development of the IAEA safety standards. The paper gives a great appreciation to all I&C experts from many IAEA Member States that have created valuable guidance for the I&C systems that can be used at all nuclear power plants worldwide.

2 IAEA SAFETY STANDARDS

IAEA has over the years conducted systematic work to create safety guidance for nuclear power plants. The present hierarchy of the IAEA safety standards involves documents at three levels; the safety fundamentals (SF), the specific safety requirements (SSR) and the specific safety guides (SSG).

Presented at the 9th International Conference on Nuclear Plant Instrumentation, Control & Human–Machine Interface Technologies (NPIC & HMIT 2015), in Charlotte, North Carolina, February 23–26, 2015.

These documents define safety principles, safety requirements, and safety guidance for nuclear power plants (NPPs). The documents provide a logical and comprehensive framework that can be applied in the design, construction, commission and operation of NPPs and I&C systems. The top document defines ten fundamental safety principles [2] that are further broken down into general and specific requirements. The specific safety requirements are further detailed into recommendations in a collection of safety guides. In addition there are many technical reports that discuss topics of importance for nuclear safety. The technical reports are perhaps not well known among I&C designers, but they provide important insights for the design of structures, systems and components important to safety.

2.1 General Requirements

The SSR 2/1 [3] defines in the Requirement 59: Provision of instrumentation design requirements for I&C systems. These should ensure that "Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant, for obtaining essential information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions and for making decisions for the purposes of accident management". Furthermore according to Requirement 60, they should ensure that "Appropriate and reliable control systems shall be provided at the nuclear power plant to maintain and limit the relevant process variables within the specified operational ranges" and according to Requirement 61 that "A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions". The SSR 2/2 [4] underlines the importance of having an I&C maintenance group to ensure the reliability and availability of these systems.

2.2 Requirements on Management and Safety Assessment

Documents on management systems sets requirements that are used in the design and construction as well in commissioning and operation. The top document is being revised, but some of its specific guidance can be found in the documents [5] and [6]. These documents give guidance on work processes and activities such as resource management, infrastructures, monitoring, self-assessments, non-conformance and corrective actions, etc. This is important especially for I&C engineers in management positions.

Another important document in this group is related to safety assessments [7]. This document provides a useful guidance on Level 1 probabilistic safety assessment (PSA). From an I&C viewpoint a Level 1 PSA provides important insights on interconnections and dependences between systems, in particular how they can influence the probability of common cause failures.

2.3 Specific Requirements

The specific safety requirements include guidance on site evaluations, nuclear power plants, research reactors, fuel cycle facilities and transport of radioactive material. The most important for I&C engineers are the SSR 2/1 for design, the SSR 2/2 for commissioning and operation.

2.3.1 Design and construction

The document SSR 2/1 has many specific requirements that are highly relevant for I&C design; chapter 3 sets specific requirements on the management of safety in the design process, and chapter 4 defines technical requirements, which include fundamental safety functions, radiation protection, design requirements, application of the defence in depth, proven engineering practices and safety assessments. Chapter 5 defines the general plant design, which includes categorisation of plant states, design basis for items important to safety, design limits, postulated initiating events, handling of internal and external hazards, engineering design rules, design basis accidents and the need to assess combination of events and failures. It also provides requirements for safe operation of the lifetime of a NPP, how human factors should be considered in the design for optimal operator performance and how deterministic and probabilistic safety analyses should be carried out.

Chapter 6 provides requirements for design of specific plants system, including a section on I&C (requirements 59 to 67). The whole chapter is relevant, because it sets requirements on instrumentations and controls for fuel, reactor core, reactor coolant, containment, steam supply, feedwater systems, turbine, generator, emergency power supply, radiation protection and supporting and auxiliary systems. The requirements on the I&C goes through provision of instrumentation, control systems, protection systems, reliability and testability, computer based equipment, control rooms and the emergency control centre.

The specific safety requirements include many general safety principles such as a hierarchy between safety and control systems and the need for operators to be able to override automatic actions. Reliability and testability are important features not only for I&C systems, but also for most systems at NPPs. A set of requirements on computer systems are targeted towards higher level systems with functions of information storage and retrieval, without consideration of specific technology applied (e.g. analogue, digital). The separation between safety and safety related systems is a requirement to ensure defence in depth. Requirements on the main and supplementary control rooms can be seen instances of the single failure criterion, for the case the main control room becomes inhabitable. The emergency response facilities are separate from the control room and the supplementary control rooms, which include the technical support centre, the operational support centre and the emergency centre.

2.3.2 Commissioning and operation

The document on commissioning and operation SSR-2/2 provides requirements for operational limits and conditions, control of plant configuration, management of modifications, periodic safety reviews, equipment qualification, ageing management, records and reports, fire safety and labour safety, which all may have implication on I&C systems. For example I&C would ensure collecting information on adherence to operational limits and conditions, plant configuration, positions of fire doors and indications of fires.

Tasks to support NPP commissioning include preparation of test and inspections programmes with detailed procedures. Requirements on operating procedures include concepts of normal operation, anticipated operational occurrences and accident conditions which include design basis accidents and design extension conditions. Monitoring of chemistry conditions and core management include their own I&C equipment. Maintenance, testing, surveillance and inspection will also need a support of specific I&C equipment. The management of outages may similarly place its own needs for signals to be collected and recorded.

2.4 Safety Guides for I&C systems important to safety

Two safety guides for I&C systems important to safety were prepared more than 10 years ago, one is covering the whole I&C area and the other software issues. Both documents relied heavily on technical documents that had been developed earlier and they are today outdated. IAEA has prepared a revision [8] which takes into account developments in I&C systems since the publication of these safety guides in 2002 and 2000. The main changes relate to the continuing development of computer applications and the evolution of the methods necessary for their safe, secure and practical use. In addition, account is taken of developments in human factors engineering and the need for computer security. The new I&C safety guide addresses the management systems for I&C design, the design bases, give guidance for I&C architecture, basic provisions for safety classifications specific recommendations for I&C systems design, the overall I&C architecture in support of the concept of defence in depth for the I&C system itself as protection against common cause failure. It has a specific section on software.

The IAEA also revised an old safety guide on the design of electrical power systems which will be published soon [9]. This is logical because reliable power supply is an important aspect of I&C systems. Power supplies are depending on I&C, because they have controls and displays in the control rooms and/or remote locations.

2.5 Technical Documents in the I&C field

One of the early technical documents [10] in the I&C field was issued before IAEA had adopted its present policy on safety standards. It had however the status of a safety guide and it was created as a major effort of the IWG-NPPCI. The document provides a comprehensive overview of important issues within the I&C area. One may even claim that this document conveys a functional structure of I&C systems that still is relevant today.

A rapid technical development in the I&C systems initiated activities within the IWG-NPPCI to bring in views on digital I&C as well as the use of software in safety related applications. Two documents were issued one on modern digital I&C systems [11] and the other on software important to safety [12]. These two documents served as the main technical basis for the old safety guides mentioned above.

3 GENERAL SAFETY PRINCIPLES

Going through the IAEA documents one can identify safety principles that are important for I&C system design. Our claim is that by explicitly addressing safety principles and their relationships to requirements, it is easier to understand how requirements relate to each other [13]. We argue that an explicit safety principle, which is applied consistently during design, makes it possible to claim that a certain types of system failures have been avoided. In the following we take some top-level safety principles and illustrate how they should be taken care of during I&C design projects. In that context we also give references to IAEA documents that sometimes explicitly but more often implicitly address specific safety principles.

3.1 Lifetime Considerations

We have selected the life cycle considerations as the first important safety principle to address, because it can be easy to forget impacts of design decisions made in the beginning of projects. For example, many early NPPs were built without a proper consideration of how they would be maintained. This resulted in additional costs during their lifetime, which could have been avoided by making components easier to access. New plants have a lifetime of sixty years or more, which means that serious thoughts should be invested to optimise constructions in view of their lifetime costs.

For I&C lifetime considerations this implies that one should prepare for two or perhaps three major modernisations during the plant lifetime. It may, for example be wise to plan for a reuse of safety requirements and application software, which requires a good level of documentation. Comparing for example the use of floor space needed for I&C equipment today, it can be seen that the same functions use only a small part of what was usual some forty years ago. A long term view weights expenditures of today against future savings.

3.2 Defence in Depth

Defence in depth is in our mind the next most important safety principle. This safety principle could actually be found already in the construction of medieval castles, they had several lines of defence, where a break in one still left another unhurt. A precondition is that the lines of defence are independent, which means that there is no single chain of events that would challenge two or more lines of defence. This principle is a major step in the applied engineering practices for safety.

In the I&C field this safety principle is adhered to by a clear separation of protective and control functions. Another consequence of this principle is that a system in a lower safety class should not have any possibility to influence functions of systems in a higher safety class. Just to illustrate how strictly this principle should be applied, one may consider a safety related system, which should report on its own state to a safety system. It cannot expect any feedback on information it has sent, because that may cause the safety system to hang up in trying to give a receipt of a successful communication.

3.3 A Graded Approach to Safety

A graded approach to safety is a very natural safety principle. A simple interpretation is that one should put more emphasis on things that are important for safety, than on issues that are less important. In nuclear power, this safety principle is supported with the safety principle that structures, systems and components (SSC) should be classified with respect to their safety importance. There are many different national classification schemes. A new safety guide has been developed (SSG-30) which provide recommendations on classification between safety, safety related and non-safety SSCs. The classification system serves as shorthand in selecting appropriate safety precautions.

Among the I&C systems the reactor protection system is in the IAEA documents viewed as belonging to the highest safety class. This means that there is a high burden on proof to show that the reactor protection system will function as intended when challenged with postulated initiating events (PIE). National legislation in some countries set quantitative reliability criteria on the reactor protection system.

The I&C systems except the reactor protection system are usually seen as safety related, which means that would not be necessary to argue for a perfect functionality. A qualitative approach regarding I&C systems is that electronics and computers typically are one order of magnitude more reliable than mechanical components, which would imply that mechanical failures are more important to consider than I&C failures. I&C failures should be taken into consideration, but it may not be necessary to use very much effort on collecting evidence for I&C safety. This statement should however be conditioned with the assumptions that serious I&C vendors have subjected their systems to a thorough scrutiny.

3.4 Design Basis

NPPs are built with some basic assumptions that govern the design and construction processes. These assumptions are documented in a safety analysis report (SAR), which provides an envelope for safe operation. This design basis contains information on main parameters of the NPP, main restrictions in operation, operating procedures, etc. that defines regions of safe operating states. It is important that this design basis is documented in large detail to be understood by later generations of owners and operators. If that requirement is not taken care of, it is possible that modifications made with the best intention are incompatible with the design basis and therefore may introduce new safety threats.

For I&C systems this threat is concrete, because the technology itself will due to obsolescence often force modifications to be done. If they are not in line with the design basis for the old I&C system there is a possibility that new hidden deficiencies are built into the systems.

3.5 Management of Failures

An important lesson from accidents and incidents is that there always will be deficiencies and failures on various levels in the system. Some calculations may fail, data may not reach intended receivers, units may go down due to failing power supplies, etc. One important safety principle in handling failures of different kinds is to make a risk analysis. The first step in a risk analysis is to identify threats and build chains of events. This may be done either forward in time by considering what for example a tube break may cause or backward in time by considering events that would be necessary to cause large fuel damages.

A risk analysis combined with the safety engineering principles of *elimination*, *separation*, *control* and *mitigation*, can propose ways to stop unwanted chains of events. An application of the single failure criterion is one important safety principle, which suggests that no single failure should be allowed to pose a threat for the NPP. The single failure criterion can be implemented using the safety principles of *redundancy*, *diversity*, *separation* and the *grace rule*. The grace rule has sometimes been called the 30-minute rule, which implies that control room crew should have at least 30 minutes time to consider their actions in an accident scenario.

For the design of I&C systems these principles are important for building barriers toward failures. A rough risk analysis can reveal a variety of failure modes, which may help implementing protective measures that minimize the effect of failures. More specifically it is relatively easy to provide digital I&C systems with advanced failure monitoring and detection functions.

3.6 Verification and validation

Verification and validation are two tasks that are present in all design activities. Generally the tasks imply that requirements on products and processes have been established. Verification means that processes and products are shown to comply with requirements. Validation in turn means that a process or product is assumed to fulfil some general goals or objectives and this is shown to be the case.

Verification and validation are closely related to raising claims and finding evidence to be used in a licensing process aimed at a safety case. This would imply that evidence is presented to make it believable that the claim is true. The evidence could depend on the type of claim, for example to be based on the results of test and inspections or through a systematic use of some safety principle in the design process. Claims that rely only on engineering judgement may however in some cases be difficult to accept. Independent assessments may in such cases provide a path towards mutual agreements between the stakeholders involved.

4 SPECIFIC I&C REQUIREMENTS

General requirements are related to management systems, specific requirements such as safety classification, design bases, risk analyses etc., are specific topics for I&C systems. Examples are the division between application and platform, architecture and software development, etc.

4.1 Application and Platform

Digital I&C systems make a clear division between applications and the platform. The application can be seen as software providing links to standard modules that are available on a platform consisting of hardware and systems software. Platforms have been developed by I&C vendors to serve in different configurations. This division implies that there is a need to consider the application and the platform as two separate entities in assessing the safety of the I&C. Confidence in software has to be built both on considerations of the software product and the software design process.

The application is always built for a specific assignment and it is therefore possible to collect information both from the design process and from the testing of intermediate products. This is usually not possible for the platform, because the design process typically took place years before the design of the application. I&C system vendors are also often reluctant to give out information on their software production processes that could be of help in building confidence in the platform.

4.2 Architecture

Modern I&C systems have a large flexibility in assigning functions to specific modules that are used for controls, protection, communication and human-machine interactions. This means that I&C design should start with a general architectural structure, which reflects needs for control and protection for specific plant systems, where the requirements given by safety classification are taken into account. This also includes the topology of communication links and a hierarchical structure of systems, subsystems and components. In establishing the general architecture it is important also to make arrangements for physical locations of equipment, power supplies, cabling etc. Establishing the general architecture one should also consider needs for redundancy, diversity and separation.

4.3 Failure Protection and Diagnostics

In the I&C design process it is beneficial to create some general philosophy for failure protection and diagnostics. Components to implement such functions can be found both in architecture design, in

application design and in standard functions available in the platform. The principles of fail safe and fail soft can be applied in the detailed application design. For diagnostic functions one may separate between failures that occur as events at some point of time and failures that develop slowly over time until some critical point is reached. With this regard, testing and testability of I&C systems is an important element during operation and maintenance.

4.4 Human-Machine Interface

Human-machine interface encompass the main and supplementary control rooms, technical support centre, the operational support centre and the emergency centres. An important aspect to consider in the design of the human-machine interfaces is a rigorous human factors engineering. The human-machine interfaces should be easy to understand and use. This can be achieved for example using mock-ups and simulators in the design process. A management systems for configuration control of the I&C in the human-machine interface is essential.

4.5 Software Design

Establishing confidence in I&C software has been one of the major concerns since the document [10] was issued. That was also the reason that the document [12] was released five years before the document [11]. Reliability requirements largely rely on a guidance that has been developed for general software design, by taking into account the specifics of the nuclear applications. The most important requirement is to apply a structured design process starting with requirements specifications and going through phases of architecture design, detailed design, coding, integration and testing. IAEA documents suggest a software design model, sometimes called the waterfall model, which has later been challenged within the software community by concepts related to object oriented programming. The differences in opinions reside in views when the coding could be initiated. Software tools that enable automatic code generation can already be used in the requirement specification phase. It is always valuable to have an initial impression of the functionality of resulting code as early as possible.

5 GUIDANCE ON SPECIFIC ISSUES

There are many technical documents that contain details on specific issues. The most important ones have mostly been integrated in the safety requirements or safety guides, but there are still documents that deserve attention from I&C point of view. Some of these documents are discussed below.

5.1 Lifetime management and ageing

Existing NPPs have a typical lifetime of some sixty plus years. Considering the I&C systems in this context is important due to two issues such as 1) technological obsolescence of I&C components and 2) I&C can help in monitoring the ageing processes of structures, systems and components [14]. Since the 1960ies the ageing of I&C systems have mainly been influenced by technological obsolescence for major systems and components. Reference [15] provides guidance on management of I&C components due to physical ageing, such as the wear and tear in normal operation and in plant transients.

5.2 Modifications and Modernisations

Modifications of the plant design or major I&C solutions may cause serious problems if they are not managed with care. The safety guide [16] gives guidance on modifications in general. This safety guide has a section on modifications made to computer based systems. When a modification is initiated it is important to make a thorough assessment of the safety impact of proposed modifications. In many cases it may be necessary to revise the assumptions used in safety analysis of the system subject to modification [17]. For example, in I&C systems, a design modification may require redesign of certain parts to ensure proper functionality of interfaces between modules.

One type of modification is the modernisations of the old I&C systems that have been carried out at several NPPs. For this specific task there are several IAEA documents (cf. [18], [19] and [20]) that provide various types of guidance. Guidance on upgrades [21] and power uprating [22] also has their own documents.

5.3 Common Cause Failures

The elimination of the possibility of common cause failures is an important task in ensuring the safety principles of defence in depth and the single failure criterion. Common cause failures may be initiated for example by physical proximity, interdependence through power supplies, cabling and ventilation, common signals, common pieces of software and common maintenance procedures. The possibility of common cause failures can be minimized by diversity. On the other hand diversity has a tendency to increase complexity, which means that some practical balance has to be found. Common cause failures are due to their importance addressed in many of the high level requirements. In addition there is a document [23] that addresses common cause failures in digital I&C systems and provisions for their management.

5.4 Security

Security is often interpreted in concepts of gates, guards and guns, but it has with the increasing use of intranets and the Internet become an important issue for I&C and computer systems. When implementing security measures it is important to understand the interdependencies between the safety and security [24]. A first step in ensuring security is to limit access to sensitive areas, which can be both physical and virtual. For computer systems it is important to ensure confidentiality, integrity, availability and reliability of the I&C systems and other computer systems [25]. The main message is that security breaks in non-safety systems also may have serious consequences on availability and accessibility of important NPP functions.

5.5 Training

The IAEA has been promoting a systematic approach to training [26] and [27], which at least in principle could be applied both for design and plant engineers in the I&C field. The document [28] gives an excellent overview of I&C systems that can be used both for initial and continued training of I&C experts.

5.6 Harmonisation

One challenge especially for I&C vendors is to understand the structure and content of national regulation in various countries. From a general point of view the reasoning is very similar, but there are also important differences [29]. In a view of the differences in safety requirements among regulators in IAEA Member States, it would be beneficial if a larger harmonisation would be reached [30]. The IAEA has an important role in this regard.

5.7 Review Missions

The IAEA has also an important role in implementation of services for Member States. Review mission for I&C systems is one such service that can be initiated on request. The review guidelines [31] have recently been established and several review missions have already been performed. The objective is to provide a comprehensive engineering review directly addressing strategy and the key elements for implementation of digital I&C systems and the use of software and/or digital logic in safety applications.

6 CONCLUSIONS

This paper describes important functions of I&C in NPPs and documents that set specific requirements on the I&C systems. It may still be difficult to form a comprehensive view of what is required. An understanding of I&C functions and requirements depends upon a larger view on how

different safety principles are connected and implemented. Our argument is that explicit considerations of safety principles can provide a path to link a large number of requirements into packages that are easier to understand and apply.

The IAEA safety guides and related technical documents illustrate the difficulty to develop and maintain a system of requirements that is both consistent and reasonably complete. In the present document structure, there are many citations from higher level to lower level documents. If there are changes made somewhere in the structure, they may introduce a torrent of changes in other documents. This has taken place in the I&C area, where the development has been very rapid.

The IAEA safety standards and related documents form an excellent pool of knowledge in the I&C area. The standards and documents have an important function to increase understanding of differences in approaches, which can lead to new and better solutions for difficult issues. The documents represent a valuable pool of knowledge. Unfortunately however terminology is sometimes inconsistent and it is not always easy to find relevant documents on the IAEA web-site.

7 REFERENCES

1. D. Fischer, *History of the International Atomic Energy Agency: The first forty years*, IAEA, Vienna (1997).
2. IAEA, *Fundamental safety principles*, SF-1 (2006).
3. IAEA, *Safety of Nuclear Power Plants: Design*, SSR-2/1 (2012).
4. IAEA, *Safety of Nuclear Power Plants: Commissioning and Operation*, SSR-2/2 (2012).
5. IAEA, *Application of the management system for facilities and activities*, GS-G-3.1 (2006).
6. IAEA, *The Management System for Nuclear Installations*, GS-R-3 (2006).
7. IAEA, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*, No. SSG-3 (2010).
8. IAEA, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, draft safety guide, DS-431 (2014).
9. IAEA, *Design of Electrical Power Systems for Nuclear Power Plants*, draft safety guide, DS430 (2014).
10. IAEA, *Nuclear Power Plant Instrumentation and Control: A Guidebook*, TRS239 (1984).
11. IAEA, *Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook*, TRS387 (1999).
12. IAEA, *Software Important to Safety in Nuclear Power Plants*, TRS367, (1994).
13. B. Wahlström, Safety principles in I&C design, NPIC & HMIT 2015, Charlotte NC (2015).
14. IAEA, *Management of life cycle and ageing at nuclear power plants: Improved I&C maintenance*, TE-1402 (2004).
15. IAEA, *Management of ageing of I&C equipment in nuclear power plants*, TE-1147 (2000).
16. IAEA, *Modifications to Nuclear Power Plants*, NS-G-2.3 (2001).
17. OECD/NEA, *Safety of modifications at nuclear power plants; the role of minor modifications and human and organisational factors*, NEA/CSNI/R(2005)10 (2005).
18. IAEA, *Modernization of instrumentation and control in nuclear power plants*, TE-1016 (1998).
19. IAEA, *Managing modernization of nuclear power plant instrumentation and control systems*, TE-1389 (2004).
20. IAEA, *Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants*, NP-T-1.4 (2009).

21. IAEA, *Specification of requirements for upgrades using digital instrument and control systems*, TE-1066 (2000).
22. IAEA, *The role of instrumentation and control systems in power uprating projects for nuclear power plants*, NP-T-1.3 (2008).
23. IAEA, *Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants*, NP-T-1.5 (2009).
24. IAEA, *The Interface Between Safety and Security at Nuclear Power Plants*, INSAG-24 (2010).
25. IAEA, *Computer security at nuclear facilities*, Nuclear Security Series No. 17 (2011).
26. IAEA, *Experience in the use of systematic approach to training (SAT) for nuclear power plant personnel*, TE-1057 (1998).
27. IAEA, *Analysis phase of systematic approach to training (SAT) for nuclear plant personnel*, TE-1170 (2000).
28. IAEA, *Core knowledge on instrumentation and control systems in nuclear power plants*, NP-T-3.12 (2011).
29. Raetzeke C., Micklinghoff M. (2006). *Existing nuclear power plants and new safety requirements – an international survey*, Carl Heymanns Verlag GmbH.
30. IAEA, *Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants*, TE-1327 (2002).
31. IAEA, *Preparing and Conducting Review Missions of Instrumentation and Control Systems in Nuclear Power Plants*, TE-1662 (2011).