SAFETY PRINCIPLES AND I&C DESIGN

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

ABSTRACT

Design of nuclear power plants (NPP) relies on the application of many different safety principles. This applies also to the design of instrumentation and control (I&C) systems, which have the important task of ensuring that the NPP never enters unsafe states. In I&C design one may separate between two control tasks, 1) to maintain the NPP in a safe region and 2) if the NPP enters an unsafe region steer it back to a safe region. These two tasks set the ultimate goal of the I&C system, which in the design process are broken down into specific sub-goals of I&C subsystems. I&C design is typically advancing from overarching abstract considerations through sequences of elaborations into concrete design solutions. The design process is governed by several more or less explicitly formulated safety principles. Some of the safety principles are general and others are specific. Sometimes there is a need to decide on which safety principle should be seen as primary in comparison with other secondary principles. Safety principles are applied in selecting design strategies, which aim at making certain failure mechanisms impossible or unlikely. In the paper I am arguing that there is a benefit of making the safety principles used in I&C design as explicit as possible as a part of the requirements specifications.

Key Words: Nuclear safety, design processes, instrumentation and control, a systems approach.

1 INTRODUCTION

The application of safety principles in nuclear power plant (NPP) design has had an important contribution to the safety of nuclear power. Safety principles have an important function as a method for selecting good and avoiding bad designs. In spite of their importance there have been only few discussions of safety principles in general. I&C systems have important functions and tasks in ensuring that NPPs will never experience accidents that endanger people and the environment. On a general level I&C systems have two functions 1) to act as an intermediary between the plant and control room operators and 2) to execute automatic controls in specified situations. These two functions may be in conflict, when either operators or automatic controls act unsafely, due to human errors or errors in I&C design.

I&C design has an important position in ensuring NPP safety. One difficulty has been the rapid development of I&C in the transfer from analogue to digital I&C. This development introduced the need for restructuring the I&C design process and the verification and validation (V&V) activities by which design errors are avoided. Especially the licensing of digital I&C has proven to be controversial in the sense that opinions between plant owners, I&C vendors and regulatory authorities seem to diverge regarding requirements to be fulfilled before I&C systems can be considered safe.

The controversies have been circling around the old question "How safe is safe enough" [1]. Especially arguments, regarding what can be considered as sufficient evidence for safety, have often been met with the argument " ... yes, but ... ". It is simple to argue that there is a need to provide proofs of I&C safety that is complete, consistent and correct (C^3). However as I will show this is both practically and logically impossible. The question therefore is not what should be necessary to demonstrate, but instead what can be considered as sufficient in a search for an increasing number of arguments that a selected I&C system is safe enough.

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.

On a general level there are two requirements that can be placed on a digital I&C 1) the system should exhibit all intended functions and 2) not exhibit any unintended function. Due to the complexity of digital I&C it is not possible to foresee or to prepare for all situations, where some defined behaviour is required. If however, the design process is structured to provide insight both into the quality of the design process and the designed product, it should be possible to agree on a sufficient set of arguments that the I&C is safe. In building the I&C design process, I think it is necessary to make an explicit use of safety principles of different kinds. In selecting and applying suitable safety principles, it should be possible to avoid design errors and at the same time collect evidence that the designed product is good enough. By making the design process reviewable by a third party it should be possible to build confidence in both the process and the product.

2 SAFETY PRINCIPLES AND THEIR APPLICATION

Safety principles have been applied in NPP design already a long time, but their application have mostly been implicit. Safety principles are closely connected to requirements placed both on the design process and on the product. In applying a certain safety principle one may argue that requirements are fulfilled and that a selected set of design errors have been avoided. An explicit consideration of various safety principles can therefore help in setting priorities and relations among requirements and in using them systematically in different parts of the design process. A safety principle can thus be of help in selecting good and avoiding bad designs.

2.1 A systems approach to safety

The perhaps most important safety principle is to apply a systems approach [2] to safety. This principle is important in all design processes, because they represent long chains of interconnected decisions, where it would be important to have some idea of the final results, before design details are decided on. Design can in this connection be interpreted broadly to encompass not only the design of a NPP and its I&C, but also the design of its management, instruction and documentation systems.

A systems approach to safety implies the use of systematic processes, where sub-processes of requirements specification, general design, detailed design, implementation and testing, follow each other in a logical sequence. It also implies that there is a management system, which is governing the design process. The management system can in actually be seen as the controller of the design process [2], to ensure that safety is the main value in the design process. Furthermore the engineers participating in the design should have a good understanding of the design process and how it should be managed to deliver results in time that fulfil expectations on quality. More concretely they should have a good understanding of risks of design errors, their consequences and methods to avoid them. The systems approach makes it possible to at the same time consider both entirety and details.

Good design has two characteristics, safety and costs. An optimal design is not maximising safety, but makes a good balance between safety and costs. Because the design of an I&C system requires regulatory acceptance, it is also necessary to make a trade-off between solutions that need an extensive process to be acceptable and solutions that are more expensive, but where acceptance may be easier to reach.

2.2 Major safety principles

A systematic application of safety principles can ensure that certain types of design errors are avoided and that good designs are selected (cf. [3] and [4]). Safety principles can be divided into two groups, where one group may be characterised as positive, "you should ... " and the other as negative "you must not ... ". Safety principles could also be arranged in a hierarchy in such a way that a primary safety principle can be assured by applying a number of secondary safety principles. More generally safety principles provide help in deciding how good "good enough" should be. A rough division of safety principles are introduced below.

2.2.1 Safety reserves

Safety reserves imply that there is room for movement and actions before dangerous limits are reached. Medieval castles were for example often built and equipped with this principle in mind. Some of the safety principles in this group that are robustness and resilience, defence in depth, safety barriers, margins of safety and fail-safe designs. An application of this principle would suggest that the state space of the system for example is divided into regions of *safe*, *danger* and *unsafe*, together with defined borders and control mechanisms that react at transfers over the borders.

2.2.2 Information and control

The systems approach to safety implies the use of information and control to ensure safety. Using the control paradigm for safety it implies the use of an objective function and a system model, together with the criteria of observability and controllability [2]. This means that there should be some qualitative or quantitative measurements of achieved safety, a model of how safety is constructed and means to influence safety. Among the safety principles in this group one may speak about experience feedback, human factors engineering, design of operating procedures, system usability considerations, operational interfaces, safety automation and risk communication

2.2.3 Demonstrability

Demonstrability has to do with the collection of evidence that the design process has the capacity to generate safe designs and that the safety principles have been applied accordingly. It also involves making experiments with intermediate and final products to demonstrate that required behaviour has been obtained. Experiments may be carried out using predefined tests or tests using stochastic inputs. Among the safety principles in this group are the use of inherently safe solutions, proven design, simplicity, inspections and reviews, building a safety case as well as ensuring inspectability and maintainability.

2.2.4 Optimisation

Optimisation has to do with situations, where two or more feasible options are available from which the best design should be chosen. Optimisation implies the existence of an order relation *better than* on the set of options. Safety principles that fall in this group are for example continuous improvements, safety quantification, agreements on acceptable rest risks, human reliability analysis, cost and benefit analysis, as low as reasonable achievable (ALARA), safety as high as reasonable achievable (SAHARA), selection of best available technologies (BAT), the substitution principle to exchange dangerous technologies with less dangerous ones, risk informed regulation, the use of safety integrity levels (SIL) and risk homeostasis.

2.2.5 Organisational principles and practices

Many safety principles have to do with the organisation of design processes. The difficulty is to get people to cooperate in complex tasks to achieve organisational goals. The use of management system is typical practice for defining goals, authorities, responsibilities, processes, tasks and activities of an organisation. Organisational safety principles are for example the use of standards and design patterns, the establishment of emergency plans and procedures for crisis management, safety management and safety culture. More generally, an organisation should at least in some sense be able to manage the unexpected.

2.3 Risk analysis and safety management

Risk analysis and safety management are two interconnected safety principles [2]. A risk analysis starts from the consideration of threats failures or errors that may start unwanted sequences of events. A threat has a probability to materialize and the resulting sequence of events can have more or less serious consequences. The probability and the consequences together form a risk measure that can be qualitative or quantitative. If risks are considered on a qualitative scale, a usual practice is to establish an order relationship between different risks to characterize their importance. For risk considered on a quantitative scale, it is usual to define a *rest risk* beyond which smaller risks could be considered acceptable.

The aim of the risk analysis is to establish broad risk regions of acceptable, manageable and not acceptable risks. Safety management can then be used to decrease the risks to acceptable levels by *elimination*, *separation*, *control* and/or *mitigation*. By elimination one could for example forbid a dangerous technology and suggest a transfer to more benign technologies. Separation can be achieved by surrounding dangerous object by fences or barriers to isolate them from the environment. Control can be achieved through the use of passive or active safety systems to break sequences of unwanted events. Mitigation encompasses all actions that are due to decrease either the seriousness of consequences or the probabilities of unwanted events that may occur in spite of other safety precautions.

2.4 Simplicity and complexity

A strive for simplicity is an important safety principle to apply in all design projects, because simplicity supports understanding, design reviews and documentation. However, the design of NPPs and their I&C is characterised with complexity. The NPP itself relies on many different technologies that should be combined to a functioning entirety. I&C is in turn cursed by the principle of *requisite variety*, which states that a successful controller has to be as complex as the system it is placed to control [5]. Simplicity both in the NPP design and in the design of its I&C system is therefore of utmost importance.

3 GENERAL SAFETY PRINCIPLES

Safety principles and requirements on design can be found among documents published by the International Atomic Energy Agency (IAEA) [6]. For example ten fundamental safety principles, which set the frame for a peaceful use of nuclear energy, can be found in the document SF-1 [7]. More detailed requirements on NPP design can be found in the document GSS-2/1 [8] and on commissioning and operation in the document GSS-2/2 [9]. In addition to these technical documents, there is an upcoming document setting requirements on leadership and management [10], which can be applied to the management system of design processes.

3.1 Lifetime considerations

Nuclear power should be seen as a lifelong undertaking for a society. Firstly the technology is highly controversial, which means that there should be a large national unity on its use. Secondly nuclear accidents carry a risk that can be very large if probability of accidents cannot be made small enough. Thirdly there should be a societal preparedness to take care of the high level nuclear waste in a sustainable manner. A NPP itself has a very long lifetime with ten or more years from the decision to build, until start of electricity production. The operational lifetime of a NPP is some sixty plus years and after that it is likely that it will take decades before a NPP site can be turn over to some other use.

This long term consideration implies that there should be some political process to ensure that a large commitment to nuclear power can be found before plants are built. One may actually require that benefits of introducing nuclear technology should be very much larger than possible negative consequences. The responsibility for the safety of a NPP lies on the operating organisation and there should be a regulatory authority overseeing the operation.

In a lifetime perspective there are several design processes in which a systems approach to safety should be applied. Processes for operation and maintenance will need their own instructions and operational limits and conditions. During operation it is likely that there will be needs for modifications and modernisations. Decommissioning and waste management will similarly have needs for activities to ensure safety. Later lifetime phases should be considered as far as possible in the design phase of a NPP, because small initial cost savings can easily carry very large costs in a lifetime perspective.

3.2 Defence in depth

Defence in depth (DiD) implies that several independent barriers against unwanted events are built and maintained. It is crucial requirement that the barriers are independent, because otherwise single events may simultaneously fail two or more of the barriers due to some common cause. The requirement for DiD appears in the requirements 3.30–3.33 of the document SF-1 and is explained more thoroughly in the requirements 4.9–4.13 of the document GSS-2/1. DiD is a principle by which a very high reliability can be built with less reliable components. Independence between the barriers can be ensured, provided that they are not coupled for example through physical location, power supplies, cabling and common maintenance procedures. It is also important to ensure that barriers have necessary support for their functioning.

3.3 Management systems

Requirements on the existence and content of management systems are given in all three documents [7], [8] and [9]. Detailed requirements are defined in the document [10] that is in the process of being published. The management systems can be seen as software for organisational control by which organisations plan, implement and assess their processes, tasks and activities [2]. The management systems should have a structure that on the highest level defines mission, values and policy of the organisation [11]. The management system should define authorities and responsibilities for organisational units and management positions. On lower levels there should be detailed descriptions and instructions for processes, tasks and activates. An important requirement is also that the management system should be reviewable and that the efficiency of the management system is reviewed at regular intervals.

3.4 A graded approach to safety

A graded approach to safety implies that more efforts should be spent on activities that are important for safety than on activities that are less important. This principle implies that there are processes for assessing risk contributions to safety of structures, systems and components (SSC) and that the risks can be ordered on an ordinal scale. This principle is connected to the requirement to establish a classification system for SSCs [12]. In the IAEA documents three classes are used, 1) safety, 2) safety relevant and 3) non-safety. National regulations differ on the number of safety classes required. In principle it would be advantageous also to classify processes, tasks and activities with respect to their importance for safety, but this is seldom done explicitly.

3.5 A design basis

A design basis is comprised of principles, requirements and documents that define a design philosophy and its implementation. It contains the safety analysis report (SAR) in which design basis threats (DBT) are defined, analysed and assessed. A DBT can be seen as a probing stone for the design and dimensioning of safety systems [2]. The design basis should also contain descriptions of operational limits and conditions, which define borders of a safe operational envelop. It is important that the design base is maintained as built throughout the lifetime of the NPP, which means that modifications and modernisations should be brought into the documents [13].

3.6 Handling of failures

The identification and handling of failures is the core of the risk analysis activity. The commonly applied *single failure criterion* implies that no single failure or operator error should lead to an accident. The single failure criterion is applied through the subprinciples of *redundancy*, *diversity*, *separation* and *grace rule*. Redundancy implies that the function of a failing SSC is taken over by a backup SSC of the same construction. Diversity implies that the backup SSC relies on a different construction or technology to compensate for design errors. Separation aims at remove risks for CCF. The grace rule or as it also has been called the 30 minute rule, is intended to give the operators in the control room time to think and act during major plant upsets. Implementation of the grace rule requires some minimum level of automation.

3.7 Completeness, consistency and correctness

Safety principles should be carried out broadly and in depth to assess various types of events and their consequences throughout the lifetime of the NPP. This means that there are requirements on the *completeness*, *consistency* and *correctness* (C^3) in threat identification and consequence analysis. Unfortunately there are no means to ensure completeness, which implies that there should be some stopping criterion for how far the analysis should be brought. Consistency with regard to the amount of detail in sequences of events may be achievable, but consistency in requirements places a demand that requirements are non-conflicting. Correctness in turn means that assumptions made in the safety analysis should correspond to reality, which is impossible due to uncertainties 1) in models used to give estimates of probabilities and predictions of consequences and 2) unknown differences between specifications and the NPP as constructed. One way to approach the C^3 issue is to agree on some tolerable rest risk that can be used to judge the sufficiency of the analysis.

4 SAFETY PRINCIPLES IN THE DESIGN OF DIGITAL I&C

The general safety principles set the scene for I&C designers. The documents GSS-2/1 [8] and GSS-2/2 [9] contain important guidance also for the I&C design process. In addition there are more specific safety principles that have to be reflected in the I&C design. These principles are discussed in two new IAEA documents [14] and [15], which are based on updates of three earlier documents.

4.1 Functions

A starting point for the I&C design is a division into functions [16]. On a general level it would mean field equipment, communication units, control units and human-machine interface units in the control room. Functional requirements on I&C systems and components come from the plant design and include reactor, turbine and generator controls as well as controls for auxiliary systems. The functional division should comply with the selected safety classification system. The result of this initial phase of I&C design should be the establishment of a design philosophy, which takes stand on general safety principles to be applied and requirements placed on various functions.

4.2 Requirements

A common division of requirements is to separate between functional and non-functional requirements. Functional requirements set targets for what the product should do in specific situations and non-functional requirements have to do with qualities that the product should have. On the set of requirements two hierarchies can be established, i.e. 1) a hierarchy of systems, subsystems and components and 2) a hierarchy going from abstract functions to concrete implementations defined on levels *why*, *what* and *how* [17]. These two hierarchies are related to each other and to stages in the design process. From there requirements specifications are developed, which should govern later stages of the design process. If for example important requirements are not identified before detailed design is entered, they may necessitate considerable and expensive changes. The requirements specifications form the basis on which the I&C philosophy is built.

4.3 Architecture

The I&C design philosophy is made concrete in the I&C architecture. The architecture should make specific assessment of necessary computing and communication capacity to allow for concrete plans for physical placement, hardware, power supplies, cabling and control rooms. The architecture should also include plans for redundancy, diversity and separation of different functions to comply with requirements in safety classes. It should suggest support and backup systems by which functionality of the I&C can be assured. For the control rooms it is important to consider human factors and the planned manning in terms of a shift supervisor and control room operators.

4.4 Application software

One part of the specifications and requirements for the application software are set in the plant design process and other parts in the definition of the I&C architecture. The control algorithms and the protection functions are determined by selecting and interconnecting available functions of the I&C platform. Self-diagnostics, failure detection and failure responses can partly be built in the application software and partly by using standard functions of the platform. One important safety principle in building the application software is to adhere to good software design principles. These include the creation of requirement specifications for functions to be implemented and to carry out necessary V&V of intermediate and final products.

4.5 Platform

The I&C platform consists of both system software and hardware. It would be advantageous if data from the platform design process has been collected, but in practice such data is seldom available. This means that there often is a challenge in establishing confidence in the safety of the platform. If good design and programming practices have been used, it would be important to provide evidence that this has been done. It may be possible to collect user experience from other installations that have used the platform. It may also be possible to design specific tests by which crucial safety features can be demonstrated. To ease the building of confidence in the platform, a strong recommendation is that I&C vendors would make data on the platform design and programming efforts available, together with operating experience collected from their customers using similar systems.

4.6 Software development

In the domain of software development there are many principles in use for ensuring software reliability and dependability. Such principles have their immediate application in developing the system software of the platform. General guidance such as requirements specifications, modular design and a stepwise integration of modules are typical for good programming principles. Modern software practices in addition call for object oriented programming, strong data types and early demonstrations of functionality. The use of computer based tools for requirements specification, code generation, configuration management and documentation are also recommended.

4.7 Configuration management

Configuration management has to do with a parameterisation of the platform software. Parameters provide flexibility in building the application, where the functionality of computational units can be changed in software. The parameterisation makes it easy to change I&C functions, but also brings a need make a thorough V&V before suggested changes are implemented. There is a need to use some computerised tool to manage the parameterisation. One possibility is to use the same tool that is used to establish a design base for the whole NPP and the other possibility is to use a configuration management system that is used for the I&C. It is also important to understand that the configuration management system is an important asset to be maintained and used during the lifetime of the NPP.

5 LICENSING ISSUES OF DIGITAL I&C

The licensing of digital I&C has shown to create controversies between utilities, I&C vendors and regulatory bodies. One issue behind the controversies are the regulatory requirements. Sometimes they are considered to be too detailed and sometimes they are considered difficult to interpret. A second issue has to do with documents that should be sent to the regulator for review, because they are often seen as an unnecessary burden in resource restricted design project. A third issue is connected to what can be considered as sufficient evidence that certain requirements are fulfilled with selected solutions.

5.1 Regulatory requirements

A nuclear regulator has two main tasks, 1) specify requirements NPPs should fulfil before licenses to be build and operate can be awarded and 2) to through inspections and reviews ensure compliance with the requirements [18]. There is a large diversity in comprehensiveness and detail between national requirements [19]. This fact often puts a burden on the argumentation that certain requirements are fulfilled with selected solutions, especially when design projects are carried out in countries from which the I&C vendor does not have earlier experience. A path to remedy this difficulty is to strive for a larger harmonisation of regulatory requirements [20].

The need to write requirements to be explicit, but not too detailed is difficult to fulfil, because requirements written in natural language will always give room for interpretations. A common observation is also that interpretations are not stable over time although the writing remains the same [21]. In principle the requirements should not be too detailed, because this may stifle a search for new and better solutions. On the other hand requirements should not have too much room for interpretations.

5.2 Reviews in the licensing process

In assessing the safety of digital I&C it is necessary to assess and document both the design process and the product. If a certain safety principle has been applied consistently in the design process, one may claim that some groups of design errors have been avoided. It is therefore important that evidence from the design processes have been collected and documented. Conjectural evidence of safety can be obtained for example from the management system used, results of inspections and reviews, etc. In addition the design itself should be properly documented.

To make the regulatory review easier a good principle is to give the regulator a description of the design process together with its processes for quality assurance early in the design project. During the design the general principle should be that important documents are sent to the regulator when they have been finalised. On the other hand the regulator should avoid requiring documents, which have not been finalised or do not exist. During the licensing process a good practice is that possible regulatory concerns are voiced early, to give time for their resolution. Regulators have been afraid to apply this practice in a fear that it could be considered as a partial acceptance of proposed solutions.

5.3 Claims and evidence

The licensing process can in principle be perceived as series of claims together with evidence for the claims to be true [22]. Each claim may contain sub-claims and evidence for them. The role of the regulator is to evaluate claims and evidence and to decide on acceptance or rejection. A rejection should be augmented with reasons at which additional claims and evidence may be presented. There is a need to use both deterministic and probabilistic claims. A deterministic claim can be based on the application of certain safety principles and evidence based on information collected from the design process. Probabilistic claims may be quantitative or qualitative. A qualitative claim could for example be that something is likely or unlikely to a certain degree.

5.4 Regulatory challenges

There are many challenges in regulatory oversight and in preparing a safety case to obtain a NPP constructions or operations license [18]. There are large differences in regulatory strategies, requirements and practices. There are also subtle differences in how deterministic and probabilistic approaches are used in the definition of acceptability. Already the fact that regulatory requirements are written in the national language of a country can trigger discussions on their interpretation.

It seems that some early digital I&C projects were started without a deep consideration of the licensing process, which implied that developers of the new technology and regulatory inspectors sometimes did talk at cross-purposes. Another difficulty seems to have been concerned with a breakdown of possibilities for a deterministic reasoning without accepting a probabilistic reasoning with qualitative evidence. There also seems to have been difficulties in maintaining a strict top down reasoning process, without a continuous reference to possibilities for common cause failures that are associated to the design process of the software.

6 CONCLUSIONS

This paper has considered applications of safety principles in the I&C design for NPPs. Similar reasoning can be used also for other types of design processes. Domains closely related are the design of human-machine interfaces in a NPP and in design of the management system that is used in operations and maintenance. An explicit use of safety principles should make it easier to obtain structural information from the design process of digital I&C that can help in applying deterministic criteria in the licensing process. This information can also make it easier to design targeted test programs by which conjectures on software functions can be statistically verified. The use of safety principles may provide an opening of some of the deadlocks concerning safety of digital I&C. I think it is necessary to open up and maintain a dialogue between regulators and application engineers within the I&C field on where the border of safety should be drawn [23]. The use of safety principles seems to be an important in such a process of discussions to establish what can be considered sufficient in the licensing process.

7 REFERENCES

1. C. Starr, "Social benefit versus technological risk", *Science*, **165**, pp.1232-1238 (1969).
2. B. Wahlström, C. Rollenhagen, "Safety management – A multi-level control problem", *Safety Science*, **69**, pp.3–17 (2014).
3. N. Möller, S. O. Hansson, "Principles of engineering safety: Risk and uncertainty reduction", *Reliability Engineering and System Safety*, **93**, pp.776-783 (2008).
4. J. H. Saleh, K. B. Marais, F. M. Favaró, "System safety principles: A multidisciplinary engineering perspective", *Journal of Loss Prevention in the Process Industries*, **29**, pp.283-294 (2014).
5. R.C. Conant, W.R. Ashby, "Every good regulator of a system must be a model of that system", *Int. J. Systems Sci.*, **1**, No. 2, pp.89-97, (1970).
6. B. Wahlström, A. Duchac, "The IAEA safety principles applied to NPP instrumentation and control", NPCI & HMIT 2015, Charlotte, NC (2015).
7. IAEA, *Fundamental safety principles*, SF-1, Vienna (2006).
8. IAEA, *Safety of Nuclear Power Plants: Design*, SSR-2/1, Vienna (2012).
9. IAEA, *Safety of Nuclear Power Plants: Commissioning and Operation*, SSR-2/2, Vienna (2012).
10. IAEA, *Leadership and Management for Safety, draft general safety requirements*, DS456, Vienna (2014).
11. IAEA, *Application of the management system for facilities and activities*, GS-G-3.1, Vienna (2006).
12. IAEA, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*, SSG-30, (2014).
13. IAEA, *Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life*, INSAG-19, Vienna (2003).
14. IAEA, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, draft safety guide, DS431, Vienna (2014).

15. IAEA, *Design of Electrical Power Systems for Nuclear Power Plants*, draft safety guide, DS430, Vienna (2014)
16. B. Wahlström, Differences between analog and digital I&C, NPCI & HMIT 2015, Charlotte, NC, (2015).
17. B. Wahlström, R. Heinonen, J. Ranta, J. Haarla, *The design process and the use of computerized tools in control room design*, NKA/LIT(85)4, Nordic Liaison Committee for Atomic Energy, Stockholm, Sweden, 110p, (1985).
18. B. Wahlström, "Reflections on regulatory oversight of nuclear power plants", *Int. J. Nuclear Law*, **1**, pp.344–377 (2007).
19. C. Raetzeke, M. Micklinghoff, *Existing nuclear power plants and new safety requirements – an international survey*, Carl Heymanns Verlag GmbH. Germany (2006).
20. IAEA, *Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants*, TE-1327, Vienna (2002).
21. B. Wahlström, R. Sairanen, "Views on the Finnish nuclear regulatory guides", http://www.bewas.fi/YVLreport_010619.pdf.
22. BEL V, BfS, CSN, ISTec, ONR, SSM, STUK, "Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorised technical support organisations", SSM 2013:08, Swedish Radiation Safety Authority, Stockhom (2013).
23. J. Rasmussen, "Risk management in a dynamic society: A modelling problem", *Safety Science*, **27**, pp.183-213 (1997).