IAEA-TECDOC-1327

Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants

Report prepared within the framework of the
Technical Working Group on
Nuclear Power Plant Control and Instrumentation

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

December 2002

The originating Section of this publication in the IAEA was:

Nuclear Power Engineering Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

HARMONIZATION OF THE LICENSING PROCESS FOR DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

IAEA, VIENNA, 2002
IAEA-TECDOC-1327
ISBN 92–0–119302–5
ISSN 1011–4289

Printed by the IAEA in Austria
December 2002

FOREWORD

This report was prepared in response to the recommendation of the Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI). This recommendation was based on the recognition of the present diversity in national practices in licensing digital I&C. The goal of this report is to promote harmonization of I&C licensing requirements in the Member States. It applies to I&C modernization, retrofits, upgrades, replacement, new installation, and other aspects of digital I&C in both existing and new nuclear power plants.

It should be pointed out that a single publication, like this report, can only take the first step towards initiating a process leading to licensing requirements, which are more harmonized. It is therefore hoped that that this report will get a broad readership among those who can influence requirements that are set on digital I&C.

This report provides general and high level recommendations to assist senior officials at utilities, vendor organizations, regulatory bodies, and their support organizations who are involved in the licensing of digital I&C. It is also intended to be read by persons participating in technical committees which are writing standards. The authors of this report believe that harmonization can be achieved through a consideration of the technical and scientific basis of high integrity digital I&C systems. It is also believed that many benefits can be reached in resolving various issues of a technical and engineering nature, which presently are creating controversies in the licensing of digital I&C in NPP safety applications.

This publication is based on a consideration of the licensing process of I&C in a top down fashion to discuss generic principles to be applied when assessing digital I&C in NPP safety applications. This report gives an overview of the confidence building process in which evidence is created that digital I&C fulfils its function. The publication presents a long term vision for how a process could be entered, which is leading to a harmonization of licensing requirements for digital I&C systems. The report is intended to provide help in resolving unnecessary differences and inconsistencies in existing licensing and safety assessment processes. This approach is assumed to ease an understanding of the engineering basis of the licensing process and therefore provide help in achieving licensing requirements, which are more harmonized.

The first consultants meeting was held in Vienna on 13–16 March 2001. At that meeting the participants developed the extended draft of the report. The second consultants meeting was held in Vienna, on 14–18 January 2002. At this meeting the final research results were incorporated into the final report.

Special thanks are due to B. Wahlström of the Technical Research Centre of Finland, who chaired the meetings, and to H.M. Hashemian, of the AMS, United States of America who along with B. Wahlström largely contributed to the report. The IAEA officer responsible for preparing this publication was Ki Sig Kang of the Division of Nuclear Power.

EDITORIAL NOTE

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The development in instrumentation and control (I&C) has been very rapid over the last two decades. New generations of digital equipment with improved performance have been introduced in the market at a high rate. This development is also reflected in new and improved systems for I&C in all major industries, including transportation, the chemical industry, and conventional power plants. The new systems take advantage of technological achievements to accommodate sophisticated and efficient treatment of measurements and control signals, for high speed and reliability, but also for flexibility and versatility.

The adoption of the new technology has, for various reasons, been slower in nuclear power plants. The most important reason is that only a few new plants have been ordered worldwide during the last ten years. A second reason is connected to the efforts needed in providing adequate evidence that the digital I&C systems can be used in safety and safety related applications. This issue is connected to the effort needed in obtaining adequate assurance that the digital I&C will fulfill its intended function and contain no unintended function in all possible operational states during its entire life cycle.

Today many nuclear power plants in the world are planning to modernize their I&C, to fight obsolescence, and also to introduce new and improved functions. For new reactor designs, there is no other alternative than to use digital I&C and the benefits of the new technology is undisputed. Practical difficulties connected to the licensing process of digital I&C have, however, shown to bring uncertainties into time and resources that have to be reserved in the projects. Various research and development projects in IAEA Member States have been carried out to establish a basis for licensing digital I&C and this has led to a situation where a large variety of national approaches have been developing. This has resulted in difficulty to define a consistent set of requirements between utilities, vendors and the licensing authorities on what requirements to place on the systems and how it can be demonstrated that the requirements have been fulfilled. In spite of these difficulties, there have been many successful projects which clearly demonstrate that the technology is mature for use in high-integrity applications. The experience base from these projects has also proved useful in suggesting methods and tools for building confidence in digital I&C.

Although digital I&C implementation and I&C modernization activities in nuclear power plants were partly motivated by obsolescence of analog equipment, the obsolescence problem will not disappear with implementation of digital equipment. In fact, obsolescence could be even more of a problem with digital equipment than it has been with the old analog equipment due to the rapid technological development in digital I&C. The obsolescence problem is often manifested in terms of difficulties in procurement of spare parts. As such, the users of digital I&C equipment must be vigilant of emerging problems and start their upgrade and modernization plans early to ensure continued operability of I&C system over the life of the plant.

In view of the diversity of existing and emerging licensing requirements, the IAEA found it useful to produce this report as a harmonizing approach to achieve a basis for licensing digital I&C in nuclear power plants. This framework is intended to encompass the licensing approaches that are presently used in different countries and thereby make it easier to understand their differences. Since there seldom are technical reasons for the existing diversity, IAEA has found it useful to explore needs and possibilities for harmonization of the

licensing requirements of digital I&C. This document is to be used for the benefit of utilities, vendors, users, regulators and their support organizations who have a need for evaluating design, development, evaluation, testing, licensing, and other aspects of digital I&C systems.

1.2. EXISTING AND EMERGING STANDARDS AND GUIDELINES

The introduction of the new technology in the nuclear power plants led to the revision of many old and the development of many new standards and guidelines. IAEA has been active in this process and several documents on different levels have been published over the years. International standardization organizations such as the International Electrotechnical Commission (IEC), the International Standardization Organization (ISO), and the Institute of Electrical and Electronic Engineers (IEEE) have also been involved in producing standards. This work is going on and important new standards and revision of old standards are in the pipeline.

In its introduction, the new technology brought along a set of issues that creates various challenges for the design and implementation of digital I&C in safety applications. Some of these challenges are:

- to create a coherent set of requirements for a rapidly developing technology,
- the long time that it takes to develop standards, which means that they may become obsolete relatively rapidly,
- the difficulty to compare detailed requirements of partly overlapping standards with each other,
- to reflect the specialized needs of the nuclear industry in the development of a new technology.

Consequently, it may in actual I&C projects be necessary to apply guides and standards, which are available still in draft version. Also, there may be situations where suitable guiding documents are not available and it may be difficult to select the most appropriate guides and standards to apply. In a situation where there is no natural guiding documents to be used, there is also the danger that a combination of requirements from different sets of standards may introduce contradictions in how they should be interpreted. The problem is thus not the absence of guidance, but rather to decide on what guidance to use and how it should be used.

National licensing authorities have, to some extent, been incorporating available standards in their requirements, but they have also produced their own requirements and guidelines. This development has reflected issues and challenges in the application of the new technology, but it has also involved an incorporation of specific national concerns. This has led to the present diversity in national licensing requirements for digital I&C, which sometimes has made the application of the new technology difficult for the parties involved in the licensing process. One issue to resolve has, for example, been how specific solutions that have been created within one system of standards could be evaluated in another system. In their refurbishment projects, nuclear utilities have sometimes found it difficult to establish and argue for a specific set of requirements used. Experience has shown that vendors sometime have difficulties in understanding and interpreting a large variety of national requirements. Finally, there have also been cases where national licensing authorities have found it difficult to understand the pros and cons of a variety of technical solutions.

1.3. SYSTEMS OF REQUIREMENTS

Requirements are typically structured to appear on several hierarchical levels. One may, therefore, speak about systems of requirements, which places some requirements on a more generic level and other at a more detailed level. The requirements thus have certain relationships with each other. Furthermore, one could also consider various more general requirements (meta-requirements) to be placed on such system of requirements. Such meta-requirements are for example that a system of technical or functional requirements should be consistent and non-contradictory. The requirements should also be formulated in a balanced way not to be too generic or too specific, because generic requirements are difficult to apply and detailed requirements may lead to sub-optimal designs. The requirements should also be efficient in achieving the goals they are designed for. Ideally requirements should be independent of the used technology, but this is seldom achieved, because the selection of a certain technology brings in more detailed requirements, which are connected to that technology.

Systems of requirements are closely connected to the design and implementation process. More general requirements are applied initially to set the stage for explorative designs, which are investigated in the light of more detailed requirements. The detailed requirements are applied later in the design and implementation process. This can also be interpreted such that the requirement levels give answers to the questions why, what, and how. Requirements will in a way define the design envelope in which designers are allowed to optimize their design. If the requirements on a detailed level are too restrictive a sub-optimal design may be the result or it may even be difficult to find a design fulfilling the requirements.

Requirements are typically used to govern the design and implementation process. The fulfillment of certain requirements can be verified by assessing both the design and implementation process and the outputs it is generating. Lower level requirements are the means by which the ends of the higher level requirements are ensured. It can also be seen that certain requirements are more efficient than others in driving the design and implementation process to solutions to fulfilling the requirements. The fulfillment of a set of higher level requirements will in a way imply a verification that the lower level requirements are efficient in achieving the higher level requirement.

1.4. BENEFITS OF A HARMONIZED APPROACH

Harmonization in this connection is understood to mean the process of making two or more systems of requirements or work practices more similar to each other. The most important goal in entering a harmonization process is to build a better understanding for differences in requirements or in work practices together with the reasons for these differences. Harmonized requirements are in this context not to be seen as more stringent or relaxed, but to be more firmly based on a scientific and technical understanding of what is needed to ensure that digital I&C fulfills its function and no other functions.

There are many benefits which could be achieved by a better harmonization of the licensing requirements for digital I&C. First, it may dissolve some of the uncertainties in the licensing process, which presently seem to make it difficult to adopt the new systems in practice. A better harmonization may also increase the vendors' base and thereby make it easier for nuclear power plants to find systems which are optimal for their purpose. Harmonized requirements could also make it easier to reuse technical solutions for a large spectrum of application and thereby make them more competitive. Harmonization could make

it easier to find independent reviewers of proposed solutions. A lack of harmonization may introduce market distortions and create difficulties in explaining adopted solutions to the public. Last, but not least, a harmonization could also contribute to the overall safety of the plants by making it possible to concentrate the licensing process on issues of real concern.

The problem in entering a path towards harmonized licensing requirements is to find consensus on issues that are considered important. It is necessary to give a proper reflection of requirements in which also local conditions are taken into account. In a process towards harmonized licensing requirements it is necessary to reflect the integrity of the licensing authorities in a consideration of their role and mission given in national legislation. Steps have been taken towards an increased consensus on the requirements on I&C systems at nuclear power plants, such as the four party consensus document and the recent common position of European nuclear regulators.[1, 2] Also, the industry has put considerable efforts to harmonize their views on design requirements on nuclear power plants in general and for I&C systems. More specifically, e.g. the American utility requirements developed by EPRI (URD, cf. Appendix B.1) and the European utility requirements (EUR, cf. Appendix B.2) for light water nuclear power plants.

1.5. GOAL AND SCOPE OF TECDOC

The need for harmonization of licensing requirements was identified at the regular meeting of the IAEA Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI) in 1999. The project to prepare a Technical Document (TECDOC) on a harmonization of the licensing processes used for digital I&C was started in March 2001. The goal of the project was to put forward arguments for a harmonization of digital I&C licensing requirements and to investigate possible routes for that end.

The goal in writing the document is to look at the licensing process of digital I&C in a top down fashion to identify generic principles that are applied when nuclear power plant safety applications are considered. The reason is that an understanding of the engineering basis for the licensing process is believed to help in achieving a harmonization of the technical and engineering requirements in licensing. It is not the intent to duplicate other documents, but to give an illustration of how generic principles are reflected in more detailed requirements. The content of the document has been based on a compromise between the two conflicting needs to make the document comprehensive and self-standing on one hand, and to make it short and easy to read on the other.

It is the intention that this TECDOC can be used by utilities, vendor organizations, regulators, and others to bring a better understanding for the need of harmonization and the route to take for approaching this goal. The TECDOC strives to provide insights in the general principles by which a proper functionality of digital I&C can be ensured. The conclusions and recommendations are intended to assist senior managers at nuclear utilities and regulatory bodies to take a stand on issues connected to the gradual process of building confidence in a licensing process. In this way, the report aims at providing guidance of a process leading to harmonized requirements and practices that are cost effective in the long run. The effort in producing this TECDOC should be seen as complementary to the efforts of International Standardization Organizations.

1.6. STRUCTURE OF TECDOC

The TECDOC begins in Section 2 with an overview of approaches for design and implementation of I&C systems in nuclear power plants. In Section 3, challenges in the

licensing of digital I&C systems are presented. This section also gives general reasons for presently applied requirements on digital systems.

Section 4 provides a vision for a harmonized approach to licensing requirements. In developing this vision, the safety classification of the digital I&C systems has a crucial position in developing a balanced set of requirements.

A basis for licensing digital I&C systems is outlined in Section 5, including a discussion of requirements set on products and on work processes that have produced them. This is followed by conclusions and recommendations in Section 6. Also, included in the report is a glossary of useful terminology connected to digital I&C systems for nuclear power plants. Finally, the report includes a number of appendices, which describe current practices of representative Member States, American and European utility requirements and an example of a classification system applied to I&C.

2. OVERVIEW OF APPROACHES FOR DESIGN, IMPLEMENTATION, AND LICENSING OF I&C SYSTEMS

2.1. GENERAL DESIGN PRINCIPLES

The I&C of a nuclear power plant is designed and implemented in close relationship with the design and implementation of systems and major components to ensure that all requirements placed on process equipment are properly reflected. The design of I&C is therefore, similar to the design in general, based on the *defense in depth* principle. According to this principle, among others, process systems are supposed to prevent unsafe excursions of the plant. Similarly, safety systems provide a second line of defense by introducing active safety measures if the plant is brought to an unsafe operational region due to equipment failures or human errors. A typical high level requirement is that the plant should meet the *single failure criterion*, which sets a requirement that no single equipment failure or human error should pose a safety threat to the plant. These general design principles are reflected in the requirements placed on the I&C.

Another general design principle which is used more generally in the design and implementation of nuclear power plants is a requirement on *analyzability*. This principle implies that it should be possible to analyze how the plant will behave in different conditions to verify that requirements are fulfilled. The analyzability principle is important in the licensing process when different pieces of evidence are weighed together in building up a safety case for the whole plant. The analyzability principle is often used in such a way that a selected scenario, a *design basis accident*, is assumed to present the largest safety threat within a certain operational envelope. Transparency and analyzability of I&C functions and systems will facilitate the licensing process.

2.2. A DESIGN BASE FOR I&C

Nuclear power plants are designed with a certain safety philosophy in mind. This safety philosophy is reflected in the more detailed requirements on various plant systems and components. The I&C should adhere to this general design philosophy and to the I&C requirements specification derived there from. For old plants this safety philosophy is not always explicitly documented, which means that a considerable effort may be necessary in order to make the design base available in a form suitable for the initiation of the I&C project.

In the case of a new plant, there might be changes in old design concepts which may require a considerable amount of thought before a proper design base for the I&C system can be established.

As a rule a design base of a nuclear power plant and its I&C systems is documented together with the safety principles applied, selected design solutions, and corresponding implications for auxiliary and other support systems. In addition there is a considerable amount of specific requirements which should be taken into account. It is advantageous if the design base is defined in functions and auxiliary functions, together with their physical implementation. Additional information in a design base includes event sequences which have been analyzed, their expected frequency, and the required functions and equipment necessary to handle them.

The plant design base is documented in a Safety Analysis Report (SAR), which also provides a kind of reference for the deterministic and probabilistic requirements to be enforced for the plant. The SAR is maintained as a living document to reflect the plant as built. The SAR is also an important document in the design and implementation of I&C systems at nuclear power plants. The SAR often contains an overall assessment of the acceptability of the design, which therefore gives a reference to the adapted general safety philosophy.

A part of the plant design base is directed towards I&C. In this connection, it is important to stress that the plant design may imply certain special requirements on the I&C which should be reflected in the technical solutions. An I&C design base will always be plant specific and it should describe the standardized type solutions used, the control room philosophy applied, naming and marking conventions, the infra-structure plan, etc.

2.3. THE CLASSIFICATION SYSTEM

The classification of functions, systems and equipment into safety classes is an important part of a nuclear power plant design and construction process. The intent with the classification is to ensure that each object is given the attention it requires based on its safety importance. The safety classification can therefore be seen as a practical approach to allocate resources during design and licensing. There are a few classification systems proposed in the international standards, but there exists deviations in the proposed safety classification. Further efforts will be required for a harmonized and consistent classification. An example of a classification of functions and systems is provided in the Appendix C.

The safety classification systems used in nuclear power plants are based on the safety philosophy and the plant design base. All structures, systems and components, including software for digital I&C, which are items important to safety, are classified on the basis of their function and significance with regard to safety. Structures, systems and components, including software for digital I&C installed and used in order to cope with Postulated Initiating Events (PIEs) are classed in the highest safety class and less important functions and equipment are classed to belong to lower safety classes. In the safety classification systems there are also principles by which the safety class is inherited from systems to their auxiliaries. The safety classifications used in the nuclear power plants today are defined in norms such as IAEA 50-SG-D3/D8 [3], IEC 61226[4], IEEE 603[5] and in national regulations.

In all safety classification systems used, there are technical and design requirements tied to each safety class. The requirements are more relaxed in the lower classes. Following this

principle, structures, systems and components, including software for digital I&C, are designed such that their quality and reliability commensurate with the safety class they belong to. The highest requirements are imposed on systems and functions belonging to the highest safety class. These systems and functions are usually restricted in their functionality, following a design principle that systems and functions belonging to the highest safety class shall be as simple and analyzable as possible. Another design principle applied is to make sure that any failure in a system belonging to a lower class will not propagate to a system classified in a higher class. Following these design principles will facilitate the licensing process. It is also important that the technical and design principles tied to each safety class are agreed on between the licensee and the licensor before the design is started.

2.4. DESIGN AND IMPLEMENTATION OF I&C SYSTEMS

I&C design and implementation can be divided into phases of specification, design, constructing, commissioning, operation and maintenance. The phases typically proceed through a few cycles of iteration, where trial solutions are checked and revised against the requirements. In that process functionality is built in at several levels using the principles of *diversity*, *separation,* and *redundancy*. An important part of the functionality of the I&C is also built in by a proper design, operation and maintenance of auxiliary functions such as power supplies, cabling, earthing, shielding, etc. The environmental conditions where the I&C is supposed to be installed are also important and have to be taken into account. Finally, a proper specification and implementation of the human-machine interface (HMI) in the main control room, auxiliary control rooms and other local consoles, ensures that the I&C system is fit for its purpose.

The design and implementation activities by which a proper functioning of the I&C is ensured varies with the phases of the project. Different technologies will also have their own needs for specialized verification and validation (V&V) methods. More generally, it can be noted that requirements typically are placed both on the product which is built and the work processes which are used to build that product. Testing and inspection are used to ensure that the required product quality has been reached and reviews and audits that requirements on work processes are fulfilled. It is also included in the requirement that all parties involved in the I&C design and implementation should have a quality system in place.

A common approach in designing I&C systems is to separate between the application and the platform which are used to implement generic and specific plant functions. This gives the benefit of splitting up the assessment process into two parts, one dealing with the generic acceptability conditions of the selected I&C platform and the other with the application oriented plant specific solutions built on that platform.

An important principle in the design is to strive for a balance between the importance a system has on safety and the efforts which are used to implement it, and to demonstrate that it is fit for its purpose. This balance gives a possibility to concentrate the efforts on those parts of the I&C which are the most important to safety. This also means that engineering judgment should be used to ensure that all reasonable efforts are made to ensure that selected solutions are minimizing threats to the integrity and safety of the I&C systems (cf. the ALARA concept).

2.5. WAYS TO DIVIDE ROLES BETWEEN UTILITY AND VENDORS

There are various ways of dividing roles and responsibilities between the utility, the system vendor, and consultants in I&C projects. The structure of the licensing process will, to

some extent, depend on this division of roles. This applies especially to modernization projects where project activities have to be fitted into the schedule of a running plant. The nuclear power plant may also set goals on the participation of their own personnel in the I&C project to ensure that knowledge and skills of their own personnel is developed and maintained. It is evident that a harmonization of technical and design licensing requirements will facilitate the relationship between utilities and vendors, e.g. facilitate reuse of software, use of standardized and licensed components and solutions etc.

Early contacts between the nuclear power plant and possible vendor companies in I&C projects are often seen as keys to success, because the utility has on one hand to explain all the requirements and the vendor on the other hand, to explain the possibilities and limitations of their I&C platform. The utilities may sometime in large projects call in consultants to write the specifications for the I&C and to participate in the design and implementation project. Sometimes the utility may for various reasons select to act as an architect engineer and take the systems responsibility for packages bought from different vendors.

There are various combinations and modifications of the schemes described above, but in all combinations the most important thing is to ensure that the specifications of the I&C system are logical, consistent, and complete. In addition, facilitating future updates, they should also be traceable and well documented. This puts a special emphasis on all interfaces both in the project implementation and the I&C itself. During the design and implementation project, it is important that the solutions are documented as the project moves along. V&V activities, including testing and inspections, are also important to carry out according to a well-defined plan. Guidance for how to carry out I&C projects can, for instance, be found in several IAEA documents such as TECDOC 1066 [6] and in several IEC-standards such as IEC61513 [7] and IEC60880.[8]

2.6. THE LICENSING OF I&C

The licensing process can in a way be seen as parallel with the design and implementation process. The licensing process has to be anchored in national legislation. The intent of the licensing process is to establish confidence in the selected solutions as described in various documents supplied to the licensor by the licensee. It is also important to build confidence between the licensor and the licensee during the licensing process. The responsibility to build this confidence rests to a large extent on the licensee. Based on the evidence provided by the licensee and the licensing conditions defined, the licensor will, after a successful process, grant the license as applied, possibly under certain additional conditions.

In implementing a digital I&C system, the utility should begin a dialogue with the regulator as early as possible. This dialogue will be helpful in getting a mutual agreement of tasks to be carried out and their timing during design, development, and testing the system.

If regulators are involved early in the process, the chance for a timely and successful completion can increase considerably. Ideally, there should be an early agreement on the evidence of functionality that is to be produced and how it should be documented during the I&C design and implementation process. During initial meetings with regulators, agreements can be reached in such areas as the V&V plan for the project and on how to ensure the functionality of the system, avoid unintended functions, etc. Such discussion could also enhance a mutual understanding of the requirement basis and thereby in the long run, promote harmonization.

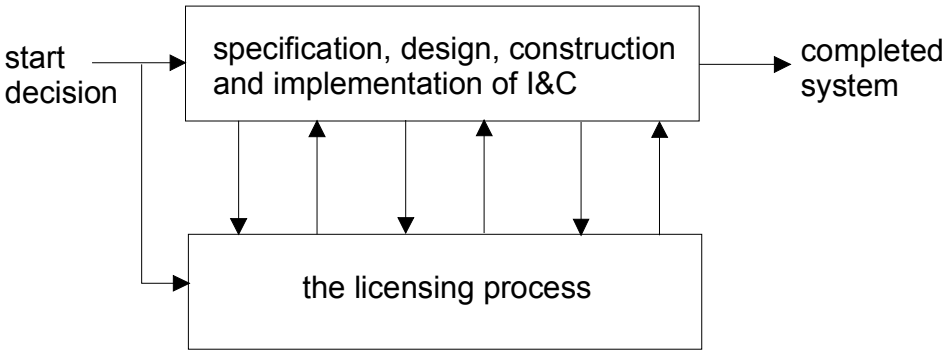


FIG. 1. The licensing process will run in parallel with the specification, design, construction and implementation process.

The licensee has the full responsibility for the safety of the plant which carries the risk that operation may be postponed until satisfactory evidence has been produced that it can be considered safe. It is obvious that the licensee must accept that responsibility and act accordingly. Therefore, it is in the interest of the licensee to verify that nothing will compromise safety and that convincing evidence can be produced that this is the case. This implies that the documents produced for the design and implementation of the I&C, including the efforts for V&V, should be comprehensive and have good quality. In principle the entire licensing is based on these documents. In practice it is necessary to allow for the time needed for the review of the documents produced by the I&C design and implementation project. It is also advisable that the safety case is documented as clearly and transparently as possible, because that will make it easier to modify the I&C at later occasions and it will also facilitate licensing. This means that the safety case should include a thorough collection and documentation of evidence that the requirements have been met together with an assessment of the acceptability of the selected solutions.

2.7. PRESENTATION OF A SAFETY CASE OF DIGITAL I&C

A Safety Case is simply a package of information describing a system, its principles, the system development processes, the V&V, and other technical, quality, and administrative details. It is usually prepared when approval is requested for a new system, a modification, a new test methodology, etc. The safety case is often included in the SAR.

The Safety Case for licensing of digital I&C equipment should describe the safety philosophy and the basic safety principles involved and how the I&C equipment comply with these principles. Further, the safety function of the systems must be clearly defined and its importance documented including the scope and functions of the I&C and its connection to the overall process. In doing so, the classification of the equipment should be established based on IAEA, IEC, IEEE or other recognized classification guidelines. The safety case should include descriptions of system requirements and specifications and outline all QA and V&V steps that will be taken. The scope and depth of the V&V should be explained together with acceptance criteria for the results of testing activities. In particular, the requirements for acceptability of the I&C system should be clearly expressed together with the justification for acceptability.

It should be pointed out that the Safety Case for a digital I&C system should go beyond the pure software aspects. Although software is the focus of the attention in digital equipment,

experience has shown that other ingredients of digital equipment is as likely to have problems as the software. A prudent approach in evaluating the system is taking a balanced view on both hardware and software.

3. CHALLENGES IN THE LICENSING OF DIGITAL I&C SYSTEMS

3.1. REASONS FOR AND CHALLENGES IN USING DIGITAL TECHNOLOGY

There are many reasons for selecting digital I&C systems in favor of the old analogue systems, which were designed in the 1970s, when many of the present nuclear power plants were built and taken into operation. These benefits include, but are not restricted to, improved accuracy, absence of drift, possibility to correlate data from different sources, possibility to store data, diagnostics and fault correction, improved HMI, etc. Most of the I&C technology today is digital and most equipment contains computers in some form or another. It has even become increasingly difficult and sometimes even impossible to find alternatives to digital technology.

The benefits of the digital technology are somewhat offset by the challenge to ensure and demonstrate the correct functionality in all possible operational conditions. The reason is that the new technology has some properties that are different in comparison with analog technology. The new technology is, for example, more concentrated and has a higher complexity for processing and communication. The analog I&C systems were, due to their relative simplicity, considered to be relatively easy to analyze and test.

This is not always the case with digital I&C because a simple software module may require extensive analysis and testing in order to prove that it, in all its operational modes, will fulfill its function and will not have any unintended functions. This means that both failures of function and unintended functions may be hidden in the system. It is essential that due consideration has been given to this possibility and that necessary steps have been taken to make the likelihood reasonably small. This requirement is valid for new designs as well as for back fitting and upgrades.

As of today, quite a number of safety applications of digital I&C exist in nuclear power plants, for example in France, Canada, UK, Switzerland and Hungary. The main difficulty with some of the first projects has been connected to overruns in cost and project schedules. This has also been very typical for large software projects in the military, administrative and telecommunications areas, which have illustrated that a learning period is connected to new technology.

A challenge in some of the projects has been the difficulty of finding an agreement between the licensee and the licensor on what should be considered as an adequate evidence that a certain I&C function is fit for its purpose. It has, in some cases, been difficult to provide evidence that design errors, which may have an influence on the functionality or reliability of the I&C, are unlikely enough. It has also been difficult to predict the consequences of such errors in advance without running the code. This has made it hard to argue against the possibility of some subtle mechanism causing failures, which may pose a threat to the integrity of the I&C system. There have been proposals that diversity in design could be used to abate this difficulty, but experience has shown that also errors in the specifications can cause CCFs and diversity in design may therefore not provide the ultimate solution.

The collective experience from the projects has resulted in the development of effective design methods, QA systems, as well as V&V methods. These systems and methods have

been documented in standards and guidelines which have been developed in parallel with the introduction of the digital I&C. Experience shows that errors introduced in the design phase are to a large extent detected and eliminated when these methods are applied thoroughly. The development of methods is a continuous effort and will eventually result in more developed standards and guidelines. An example is a new project undertaken by IEC TC45 with the title "Design of I&C Systems Important to Safety to Cope with Common Cause Failure".

3.2. FAILURE MECHANISMS AND FAILURE MODES IN DIGITAL I&C

The properties of digital I&C requires special precautions and the following failure mechanisms and failure modes must be taken care of in order to assure that the safety requirements are met without dependencies from the new technology:

- CCF due to errors introduced in the requirements specification and design phases.
- Failures caused by environmental influences, e.g. electromagnetic interference.
- Faults during maintenance and modifications.
- Failure caused by unauthorized system access.

The dominant failure mode of digital I&C is deterministic and not stochastic and therefore the same arguments with which high reliability analog systems have been built cannot be used. It is clear that there is a similar possibility that design or maintenance errors can produce similar common cause failures in the old analog systems, which also has been demonstrated by experience. The new systems are, however, more complex and therefore it can be argued that there is a larger possibility that errors go undetected. The complexity makes it more difficult to identify all interactions between software modules, especially when unexpected signals or hardware faults trigger them. Experience from software development has shown that these interactions should be specified in large detail and all intermediate steps in the software design process needs to be thoroughly inspected and tested to yield the required high functionality.

Another challenge in digital I&C is that it is not enough just to consider a failure of function. It is equally important to consider the possibility of unintended functions caused by persistent design errors that are triggered by unintentional or intentional interactions with the systems. Digital I&C systems are also somewhat more sensitive to environmental influences such as temperature, pressure, electromagnetic interference (EMI), accelerations, etc. Failures can be introduced both during operation and maintenance and especially changes and modifications have shown to be error prone. Last but not least, failures can also be caused by unauthorized system access. All these failure modes have been identified and if they are thoroughly considered in the design phases, they should not pose threats to an error free function of the system.

Experience from the use of digital I&C in the nuclear industry, as well as in conventional industry, shows that in many cases failures have wrongly been blamed on the use of the digital technology. In most cases, the root-cause of a failure is found in the requirement specification or in the prerequisites that have been used for writing the specifications. Experience also shows that errors introduced during the design and implementation phases have been the root-cause in very few cases provided that good engineering practices have been used.

The errors introduced in design and implementation are, to a large extent, captured by the application of effective V&V. Failures introduced in the specification phases are not only difficult to detect, but they are also introducing the risk of CCFs, which cannot be decreased using redundant hardware. Because of this, and in comparison with analog I&C, the complexity of digital I&C requires those larger efforts to be allocated for writing and reviewing the requirements specifications. It is also a common recommendation to use formal methods whenever applicable and when such methods are available.

3.3. HOW TO COPE WITH UNINTENDED FUNCTIONS AND OTHER FAILURE MECHANISMS IN DIGITAL I&C SYSTEMS

Besides writing good requirement specifications, use of formal methods, use of effective methods in design and V&V and the application of effective QA routines, separation between application and system software, etc., it is recommended that various barriers be used in order to cope with unintended functions and other failure mechanisms in digital I&C. Examples of barriers used to cope with e.g. failure of functions are:

- extensive self-diagnosis,
- switch over to stand-by units,
- cyclical execution of the software.

An assessment of the efficiency of these barriers is an essential part in the assessment of the functionality of the whole system. This assessment may sometimes require extensive resources, because functions built in with the aim of an increased safety and reliability will, in some cases, make the function more complicated, e.g. failure correction functions, self-diagnosis functions, etc.

If many functions are allocated to the same hardware, the vulnerability of the system increases since several I&C functions may fail at the same time. To minimize the consequences of hardware failures in safety applications, only well defined and confined software functions belonging to the same safety class are allocated to the same hardware. Of the same reason is communication between I&C functions of different safety classes restricted to go in one direction, from functions with higher class to functions with lower safety class.

In order to avoid that unintended stops of the execution of the software code (software hang-up) takes place without indication, the system software is provided with a watchdog function. The watchdog function will, as a minimum, alert the operators by an alarm.

Protection against unauthorized system access can be achieved by means of different combined measures as e.g.:

- Physical protection by means of adequate spatial installation in locked rooms and cabinets.
- Restricted access by qualified authentication procedures.
- Protection by the use of firewalls, application of specific gateways and or application of cryptographic procedures, etc.

Sometimes it may for operability and also for safety reasons, be beneficial to introduce remote access to data from the I&C. For instance, for the purpose of software maintenance

and remote diagnostics. Presently, such functions that offer outside access to vital safety systems are discouraged.

Finally, it is important to have a configuration management system in place to ensure that different software versions are compatible, that the correct version is running, that changes are traceable, etc. All items of software development, such as compilers, development tools, configuration files, application software, and operating systems are normally under configuration management control. The management control will prevent the operation and use of old or incorrect versions of the software, thus preventing failures to occur.

3.4. IMPLICATIONS ON THE LICENSING OF DIGITAL I&C

Because it is practically impossible to demonstrate a complete absence of errors in software, the arguments in the licensing have to be built in a different way. A very careful design process, together with a good quality system, can make it unlikely that errors are generated and that the errors, which are made, are likely to be detected. The collection of statistical information on errors found in the software since its release can provide important evidence in the confidence building process. The application of, for example, Failure Mode and Effects Analysis (FMEA) during design and testing can make a believable argument that possible errors will not have major effects on the functionality of the I&C. The operation of the same software on the same but redundant hardware with different data streams can support the argument that the likelihood of CCFs is small. A well prepared V&V program which includes extensive test of single software modules as well as the integrated system can support an argument that no data combination is likely to cause a major break down of the system.

The need for collection and use of evidence of quality along the software design process puts a considerable requirement on planning the design and implementation of the digital I&C beforehand. Otherwise, it may not be possible to collect and document the necessary data from the design and implementation process in a systematic way. This has to be done during the design of both the I&C platform and the application hardware and software. For those parts of the I&C which rely on Commercial Off The Shelf (COTS) products such as processors, compilers, operating systems, etc., this information may not be available, but then it may be possible to argue that the collected operational experience from those products can be used as evidence for quality. This experience is, in some cases, not appropriately documented to be used as evidence for proper functionality. Additionally, it is essential that such products are used in a conservative way to ensure that they are applied within their intended design envelope.

Perhaps, the most important advice both in the design and implementation of I&C systems and in software development is to develop specifications which are detailed, non-contradictory and complete. An early investment in the specifications will most likely pay off later in a higher reliability of the system and an easier process of providing evidence that the reliability has been reached. Specifications that initially are of a good quality are a large asset in any project, because late revisions of the specifications are always error prone.

3.5. APPROACHES TO GENERATE EVIDENCE OF AN ACCEPTABLE QUALITY OF SOFTWARE

Approaches by which evidence can be generated that software has an acceptable quality are considered in the guidelines and standards of good software practices. Perhaps, the most

important overriding principle is *simplicity*. This principle leads to modularization and the use of structured design methods. Sometimes the urge for failure detection and recovery may introduce additional complication and error proneness. It is also in line with good design principles to have well-established quality systems and to use a system of independent assessments and reviews.

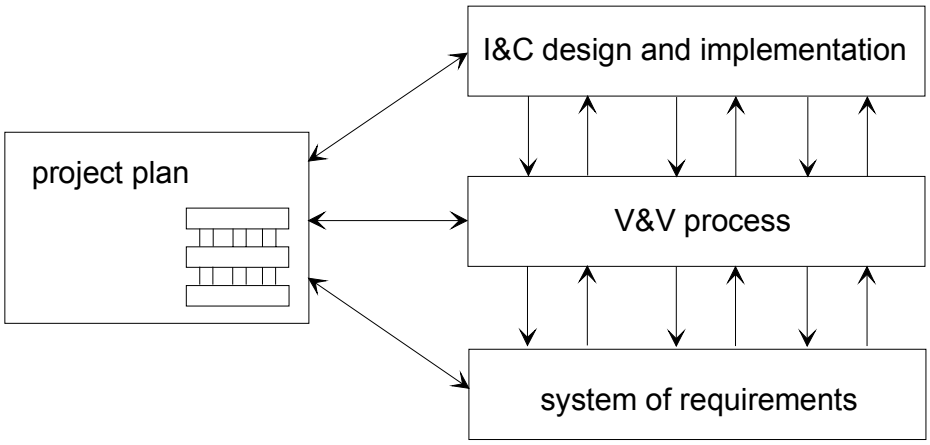


FIG. 2. Importance of a project plan.

There are a large number of computerized tools available both for the design and analysis of software and the support given by these can be very valuable both in the design and the licensing processes. Finally, there are a large number of different testing methods which can be used to gain additional confidence in the quality of the systems. The use of computerized testing tools can also ensure coverage, which is not possible with manual methods.

The process of generating evidence that a certain solution is fulfilling all requirements cannot for digital I&C rely on a single method or test. This actually implies that all methods and tools used should be integrated in a confidence building V&V process where different pieces of evidence are integrated. Again, the implementation of such a process is not possible without an initial plan to carry out the V&V process. According to the more general principle of confidence building throughout all phases of the project, one important component is confidence in the V&V plan. This implies that the plan has to be assessed and accepted in order to provide a reasonable assurance that the I&C system will fulfill all its functions and will not contain any unintended functions.

3.6. ENSURING FUNCTIONALITY OF COMPONENTS AND SYSTEMS

The separation between the I&C platform and its application has the potential of making the licensing process easier by separating between two parts which often require different specialization. If the same I&C platform is used for different applications, it is possible to reach more cost effective solutions, because licensing costs may be shared between two or several projects. It may even be possible to arrive at a generic acceptance of a platform for a range of applications. In other cases, a third party review of a specific component with embedded software may be used to certify the product for some specific purpose in a type testing procedure.

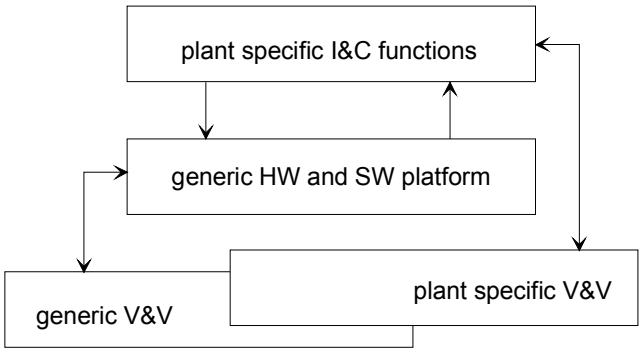


FIG. 3. The separation between plant specific functions and a generic.

Systems testing is at some point in time to be performed using the target hardware with the correct software configuration. According to standard practices this is at least done at two occasions, first at a Factory Acceptance Test (FAT), and secondly at a Site Acceptance Test (SAT). These tests are preceded by many other tests in various configurations and at various occasions. The FAT and the SAT should, in principle, be allowed to generate only a few errors or anomalies. [9]

The coverage of the tests should always be evaluated at least qualitatively, because the test should at least in principle exercise the system in all possible operational conditions. This implies that the environmental conditions, various failure modes, and unauthorized access are defined within the testing program. V&V together say: "Did we do the right thing and did we do it right?"[10]

3.7. A COMBINATION OF APPROACHES FOR SPECIFIC APPLICATIONS

The challenges in licensing digital I&C implies that the licensing has to be based on a gradual confidence building process between the licensee and the licensor, where all possible evidence is collected moving along in the design and implementation project. This means that deterministic and probabilistic requirements are combined during the process. One may, for example, argue that a certain failure mode can be considered unlikely due to special deterministic conditions that have been used during the design and implementation process. One may also, for certain functions, argue that the application software can be considered deterministically correct if it is simple enough and thoroughly inspected. The arguments that are likely to be used should be spelled out in a V&V plan of the I&C design and implementation project. QA procedures and quality systems can give guidance in this respect. The V&V plan should also specify why the arguments can be considered reasonable in the assessment of the digital I&C. The V&V plan will therefore, in practice, provide the most important document on which the acceptability of the digital I&C and its software solutions will be based.

In practical application projects there are many techniques in I&C design to increase reliability of function through the application of *diversity*, *redundancy,* and *separation*. For the most demanding application, it may, for instance, be motivated to use diverse I&C to implement the same or diverse safety functions. The credit, which may be given for various reliability increasing techniques, will vary from case to case. It is important that the reasoning behind the acceptability of a certain solution is documented very explicitly.

If there is a need to provide a quantitative reliability estimate for some certain software based safety function, there is a formal method, Bayesian Belief Networks (BBN), by which evidence coming from different sources can be combined. This method can be used to weight together, for instance, qualitative evidence such as assessments of test coverage with quantitative evidence coming from error reporting. Even if the data is not always available, it gives a sound basis for reasoning on how evidence can be combined. The method is practical for use only in the most demanding safety applications.

3.8. PRACTICAL ISSUES IN THE LICENSING PROCESS

In addition to the more fundamental issues in ensuring a proper functionality, there are a number of more practical issues which have to be used in the confidence building process. One issue is connected to the complexity of the systems and how a proper knowledge and skill is maintained within both the design and the review part of the process. There are many different disciplines to be covered and therefore it may be difficult to find experts who have both a broad and deep understanding of all issues involved.

Another issue is connected to the need for re-licensing a modification of the digital I&C. For example, it is clear that the change of a single parameter should be considered as a part of normal maintenance and therefore governed by the QA procedures. The installation of a new version of software has however, sometimes caused that many problems that a more thorough assessment may be warranted. A good and comprehensive configuration management system facilitates such assessments. Maintenance and future changes should be taken into account already in the requirements specification phases. If, for example, executable code and data are stored in separate physical memories future changes in a database could be considered not to require any functional tests since the change can be performed without affecting the storage of executable code. Finally, if the specifications for the software are changed, it seems prudent to require appropriate V&V and re-licensing.

It is always difficult to define the border for acceptability in a spectrum of technical solutions. The trade-off between visibility in the design process and operational experience is also a difficult issue. It is clear that the more stringent requirements in higher safety classes can be relaxed in moving to lower safety classes, but the question is how much. In the process different pieces of evidence has to be interpreted and weighed. Finally, it has to be agreed what kind of material should be supplied to the authority in the licensing process.

The licensing process will always imply that engineering judgment is exercised. This can for example be the weighting of the possibility that safety threats still are contained in the I&C against evidence that these threats have been removed. This kind of expert judgment cannot be exercised without a theoretical understanding of various failure mechanisms together with practical experience of their frequencies from practical projects. Therefore at some level it is important also to support a collection of experience from digital I&C at the broadest level possible.

4. A VISION FOR A HARMONIZED APPROACH TO LICENSING REQUIREMENTS

4.1. INTRODUCTION

The licensing processes have to be connected to the legislation in the country in consideration to reflect local conditions and practices. National requirements typically have a history, which is based on an industrial tradition, and the way nuclear power was introduced.

Thus, a variety of national requirements were created, sometimes perhaps even with the intention of protecting specific national interests.

Considering today's situation where utilities own nuclear generating capacity in several countries and electricity is sold over national borders, the need of harmonizing the licensing requirements becomes evident. It would improve the comparability of technical solutions and the assessment of the associated safety issues, which in turn would help to enhance economy and optimize the plant safety. At the same time, the licensing processes and the assessment results involved would become more transparent to the public. In an advancing globalization of the power industry one aim of the harmonization is to get rid of seemingly diverging licensing decisions (from one country to another), whose technical basis is not understood and which in this way inherently generates uncertainties if technical problems really exist and how they should be approached.

In essence, it has to be concluded that today there is no technical or scientific motivation for the variety as seen in the national licensing processes. Experience has also shown that national regulators sometime have difficulties to understand the requirements in neighboring countries. Finally, it would also be in the public interest to ensure that national regulation is transparent and understandable. In a strive for more harmonized approaches to licensing, one way could be to establish a set of general principles including an agreed terminology and phrasing, instead of detailed requirements, with the aim that they can remain invariant for a longer time period.

A development towards increased harmonization has to build on a harmonized technical requirement base. Work within IAEA, utility organizations, standardization organizations and the authorities has aimed at a common understanding of requirements through dialogue and attempts to reach consensus on the high level safety principles and requirements. For example, the requirements as defined by the European utilities requirements (EUR), which are addressed to the designers and suppliers of LWRs, aim at the harmonization of items like the safety approaches, targets, criteria, and assessment methods as well as design objectives and equipment specifications. Thus, not only a basis for the procurement of plants is provided, but moreover a harmonized technical licensing basis by:

- setting common safety targets which are consistent with international objectives,
- promoting common technical responses to safety issues,
- establishing requirements that are considered valid across all countries in the world.

The Nuclear Safety Convention has initiated a dialogue between authorities in different countries to achieve a shared understanding of how various national requirements relate to each other. More recently the West European Nuclear Regulators Association (WENRA) started its activities and it is to be expected that an important impact on harmonization of licensing will be provided by this organization. It would be beneficial if this kind of dialogue can be extended also to the digital I&C.

In aiming for harmonized licensing requirements it is also necessary to consider present development trends in the digital I&C. Some of these trends today are open interfaces, embedded software, COTS software, and common system platforms. It is also likely that future development will move towards an increased use of various software tools. It is to be expected that the rapid development in electronics, computers and communication technologies will continue at least for the near term future. This may imply that the systems, which are in use today, are becoming obsolete only in a few years. When this development is

reflected on the expected operational life of nuclear power plants, the I&C is most likely to be modernized several times during the lifetime of the plant. It can also be assumed that modernization projects and the construction of new reactors will rely on the utilization of information technology during design and construction. It may even be expected that in the future, the I&C design and implementation is integrated into a frame of plant information management scheme that has a plant life time perspective. Such an approach would cover systems and equipment such as instruments, cables, signal conditioning, control rooms, human-machine interfaces, control equipment, process computers and other real time computers. Such a development also places a concern on how the quality of these systems can be ensured.

To account for the technical development, it is necessary to develop a long term strategy for the I&C in which obsolescence and aging of equipment is managed. For this purpose it would be necessary to have some general model on how to allocate resources wisely throughout the I&C life cycle. Such a model could also identify various parts of the I&C design and implementation project to predict resources and controls needed in various phases. It seems obvious that only a reuse of the original design to the largest extent possible, can be cost effective if the I&C has to be exchanged several times during the lifetime of a nuclear power plant. This can be achieved only if the I&C specifications and software design to a large extent can be made independent from the used hardware. Since the digital I&C systems today are distributed modular systems, there is the potential to define software modules which can be re-used without any changes. In order to achieve this goal, a careful planning of the I&C design and implementation process is necessary.

4.2. GENERAL CONSIDERATIONS

Any attempt to build a consistent set of licensing requirements has to rely on a general safety philosophy which is used to define lower level requirements. The details of the licensing process could then be agreed on a case-to-case basis between the licensee and the licensor. A general safety philosophy can, for instance, be found in the high level documents like the IAEA safety fundamentals and safety guides. These high level documents have to be applied when the I&C project is set up and the I&C requirements specification is to be written. In the process of applying higher level requirements to the construction of lower level requirements, it is important to document their mutual relationship and connections to technical solutions. This would also illustrate how the requirements are driven by the general safety considerations.

The full responsibility for safety is laid on the licensee and it is therefore obvious that the plant owner has an interest in being serious in fulfilling not only the safety and licensing requirements, but also the operational requirements. For I&C, quality problems typically demonstrate themselves through problems of availability which have a direct influence on plant safety and economy. Therefore, it is in the interest of the licensee to require at least the same, if not more, evidence as the licensor that the I&C is fulfilling its function.

Similarly, it is in the interest of the licensor to ensure that the licensing process does not interfere with the design and implementation process to cause an unbalanced distribution of resources from a safety point of view. It is also important to reach a balanced approach over what has to be done in the evidence and confidence building process This implies that there should not be hidden catches in the licensing process, which, for instance, could make it impossible to continue just for some formality reason without any real influence on the safety. It is clear that both the licensor and the licensee have an interest to make the licensing process a supporter of good solutions and not a hindrance.

4.3. SYSTEMATIC REQUIREMENT SCHEMES AS AN AID FOR HARMONIZATION

Consistent top-down design approaches that provide basic principles as a starting point and structured step-by-step detailization of the specifications constitute a solid basis for harmonization. One possibility is the safety goal approach which is widely used. On top the safety goals are defined (control of reactivity, cooling of fuel elements, enclosure of radioactive substances, limitation of radioactive exposures) based on which the safety functions to meet the goals are developed and classified according to their importance to safety. This implies the possibility to grade the functional requirements accordingly. In the course of designing the implementation of functions into systems, the system qualification will be matched to the safety importance of the functions. This procedure provides a clear connection between the requirements on the functions and the requirements on the associated systems and equipment of the plant. It has also been proven practical because sub-systems often carry functions of different safety importance. [4]

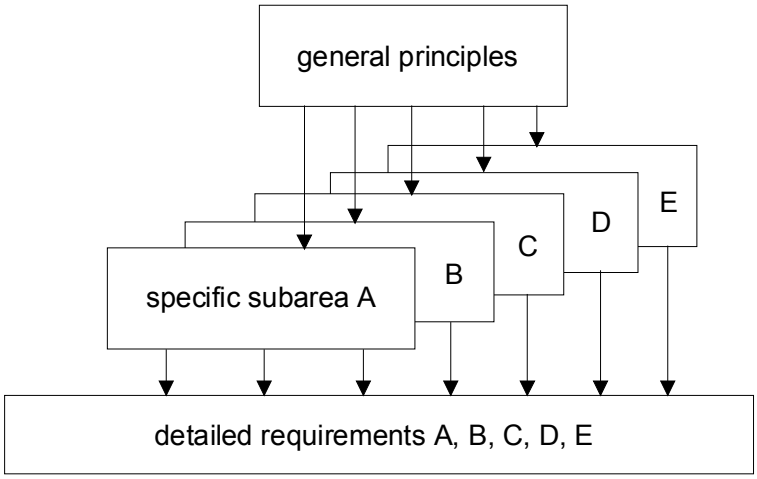


FIG. 4. Structure to provide a traceable path between general principles and detailed requirements.

Consequently, the classification system carries the requirements connected to different safety classes on how the design and implementation of I&C should be performed. Typically, requirements are set both on products and on work processes. The classification system carries the requirements used in the licensing process and the evidence to be presented so that the solutions are acceptable. A common safety philosophy is the most important prerequisite for harmonization. To build a classification scheme on these might be considered as to cause no problems, but practice has shown that it sometimes is difficult to agree upon a common classification, which however would be important in easing the discussion and achieving harmonization.

Presently there seems to be a fair agreement on the requirements to apply in the most demanding safety classes. There seems, however, to be less consensus on how these requirements should be relaxed in the lower safety classes. Additional clarifications may therefore be more urgent in the lower safety classes in approaching a path towards increased harmonization.

The concept of postulated initiating events (PIEs) has an important connection to the classification system. Functions necessary to cope with PIEs are an important part of the defense in depth design strategy as applied in all nuclear power plants. The functions needed to cope with disturbances and accidents place certain requirements also on the I&C system and its auxiliaries. The requirements to apply are typically based on a deterministic and probabilistic reasoning on what may be considered as a reasonable design target.

In modernization projects there is often a need for interfacing old classification systems with newer ones. It seems however difficult to create generic principles for how this should be done, which means that they are necessary to handle on a case-by-case basis. Experience from projects where a reclassification of functions and equipment have been attempted, illustrates the difficulty of combining two philosophies in a logical and consistent way.

4.4. BENEFITS OF A HARMONIZATION OF LICENSING REQUIREMENTS

If an approach for harmonization of licensing requirements can be reached, one could expect a higher reliance on international agreements and standards. This would ease the burden placed on national regulators, because it is a large effort to maintain national requirements up to date. A harmonization can in this way support a better transparency of the licensing processes. In order to achieve harmonized requirements, a good description of relationships between different requirement systems and between different hierarchical requirement levels is a prerequisite. If the requirements were traceable it would be easier to maintain them during a rapid technological change.

A harmonized requirement base and harmonized work methods can be expected to ease the work of all parties involved in I&C projects. Most importantly, a harmonization has the potential to decrease uncertainties in the estimates of time and resources to be used in the licensing process. A better harmonization may also increase the vendors' base and thereby make it easier for nuclear power plants to find systems which are optimal for their purpose. Harmonized requirements could make it easier to reuse technical solutions for a large spectrum of application and make them more competitive. Harmonization can also be expected to support the development of competency on a global basis to support the resolution of the really hard parts of providing evidence that certain solutions are acceptable. Finally, harmonization can make it commercially interesting for companies to create specialized tools for design and verification of software to be used for digital I&C application in nuclear power plants.

One special challenge for digital I&C in the nuclear industry is connected to the lower safety classes where standard equipment developed for the conventional industry may be applied. The nuclear industry itself has difficulties to collect the necessary experience base, which is needed for high reliability equipment. It may also be argued that producing special nuclear-grade equipment in short series may not necessarily be more reliable than standard industrial products produced in long series. A harmonization of views seem to be necessary in order to make it possible for the nuclear industry to make proper use of the experience base of the conventional industry.

It can be assumed that a harmonization will lead to better understanding of the roles, tasks and actions of utilities, vendors and authorities in I&C design and implementation projects. This would in a longer run, hopefully, result in decreased costs and better predictability in the projects, and also in addition increased safety through efficient work processes and a reusability of the technical solutions in the digital I&C systems. Finally, a

harmonization of licensing requirements may also make the licensing process more transparent and understandable for non-experts in I&C technology.

4.5. HARMONIZATION OF THE I&C LICENSING APPROACH

Ideally, a set of licensing requirements would cover both technical and administrative requirements. Typical technical requirements are for instance requirements on separation, redundancy, and diversity. Administrative requirements are usually placed on the quality system and on procedures for change management. A separation between technical and administrative requirements is related to a separation between requirements set on the product and on the work processes. This separation is often not clear in standards and guidelines for digital I&C.

A harmonized licensing approach cannot be achieved if it is not systemized and described in enough detail. This means that requirements set on I&C functions should be described beforehand and they should be anchored to the more general design principles and requirements which have proved efficient in achieving an acceptable safety. This also implies that there should be a clear statement for credits, which could be allocated to various technical arrangements such as diversity, separation and redundancy at different hierarchical levels of the system.

An important part of the path to an increased harmonization is through the creation of a better understanding of and consensus on the technical requirement base on which standards and guidelines are built. If a standard or guideline has a clear relationship to commonly accepted design principles and systems of requirements it is easy to agree on its use. If standards and guidelines could be written to be functional, i.e. to be more independent of technical solutions they are also more likely to be stable over time.

There are some practical approaches which on a relative short term can support a better harmonization of the licensing requirements of I&C. There is a need to create agreed concepts and terms used. Secondly, there is a need for a generic model for how I&C design and implementation projects are carried out. This is to some extent done in the creation of standards and guidelines, but it may be necessary to lift these efforts to a more generic level and also to describe how such generic models are converted to guidance for actual projects.

In the development of harmonized approaches it may be necessary to identify specific sub-areas of I&C where there seems to be little disagreement. These sub-areas could then be left more aside to concentrate the efforts of reaching a consensus in areas where there is more disagreement. There are various fora for such discussions where also additional efforts can be initiated. The IAEA TWG-NPPCI and IEC TC45 provides for instance established channels through which various needs can be discussed and the creation of new documents can be initiated.

5. A BASIS FOR HARMONIZED REQUIREMENTS

5.1. INTRODUCTION

In this section some requirements are discussed that are independent of national conditions and at large undisputed. For example, there is a large agreement that digital I&C system should be implemented using sound design methods and good quality assurance practices. This implies, for instance, that the following characteristics are addressed:

- Simplicity.
- Reliability.
- Robustness.
- Fault tolerance.
- Self-diagnostics.

As importantly, protection against CCFs is a common goal in the design of all digital equipment for important applications in nuclear power plants. Barriers should be built in the design and specification of digital I&C systems to break consequences of failures as much as possible. The use of diversity, separation, and redundancy are examples of technical means that should be implemented to protect against CCFs. A good design process and V&V are equally important.

These very basic requirements could be the starting point for the harmonization of licensing requirements, together with other important requirements on products and processes. Examples of such well-established requirements, independent of national conditions, are provided below.

5.2. SOUND DESIGN PRACTICES

As digital I&C systems for important applications in nuclear power plants are normally complex, modularity should be used as an approach to cope with system complexity. That is, the system should be broken down into modules that are designed, verified, and tested separately before they are integrated to larger entities. An advantage of modular design is that hidden faults are easier to reveal and correct.

There are many advantages of modular designs, but also a few disadvantages. One disadvantage is that modular designs require interfaces that are used to integrate the individual modules to construct the whole system. The interfaces are places, where problems often occur as interfaces usually are difficult to specify, code, assess, and test. As such, the designer should attempt to limit the number of interfaces as much as possible.

An I&C system must interface not only within itself but also with other systems in the plant. Experience has shown that care must be taken during the digital I&C system design to handle the interfaces prudently to minimize the possibilities for errors. More specifically, the requirements for design of interfaces shall be specified thoughtfully to ensure successful I&C system integration, operation, and reliability.

Taking advantage of new technologies such as computer aided design, object oriented programming, and other computer tools are recommended in design, development, and testing of digital I&C systems. These tools will be helpful in keeping potential human errors to a minimum.

5.3. REQUIREMENTS ON PRODUCTS AND PROCESSES

An obvious product requirement is that an I&C product is fit for its purpose. That is, the requirements for functionality, reliability, and other system characteristics should be in tune with the intended use and the location of the system. For example, the requirements for environmental conditions around the product should depend on where the I&C equipment will be installed. This is especially important if the equipment is required to function in a harsh

environment during or after an accident. A number of standards and guides are available under the subject of *environmental qualification* to assist in this area.

Another obvious requirement for a digital I&C product is that its operating system must be reliable especially if the operating system is shared by a large number of applications. In particular, the software must not produce unintended functions. Therefore, in addition to careful design and good QA plan for the project, thoughtful measures should be taken to ensure that unintended functions are not brought into the code. A separation between different parts of both the software and the software development process can help in this respect. A careful review of the source code by independent reviewers is also an important step in a series of attempts to ensure software dependability. Furthermore, a thorough V&V program should be prepared and executed for the software to catch errors that may produce unintended functions.

It is important to ensure that the functionality of the I&C is not lost in any situation and that such losses are detected in a timely manner. This objective can be reached by a combination of different activities. Good coding principles of the software with accurate error handling is one component. A definition of allowable variation range for variables is another. Finally during Factory Acceptance test (FAT) and Site Acceptance Test (SAT), measures may be taken to not only test for functionality of the system, but also verify that unintended functions are not generated. Furthermore, it is important to demonstrate the functionality of the I&C system during all operational conditions. Therefore, the system should be tested in various operational modes such as normal operation, disturbances, and simulated accident conditions.

Additional important activities should include the following:

- Periodic Tests to Ensure Continued Functionality.
- I&C Aging Management.
- Configuration Management

It should be pointed out that above measures may or may not be all that is needed to ensure proper implementation of digital I&C in nuclear power plants. They are, however, among the most common measures that the nuclear and other industries have taken in implementing digital equipment. What is important to note is that a balanced approach is essential. A balanced approach will not allow one to over-emphasize one aspect of the design, testing, or implementation at the cost of neglecting another aspect. For example, software V&V is very important in implementation of digital equipment. However, preparation of proper technical specification for the system is also very important. Therefore, in planning an I&C implementation project, the effort must be distributed appropriately. For example, an extensive testing of software can never compensate for poor technical specifications.

5.4. QUALITY ASSURANCE

As mentioned before digital I&C implementations in nuclear power plants should involve a quality management system. This implies that the work should be performed under a formal QA program covering the whole life cycle together with all typical ingredients of such a program such as formal procedures for important aspects of the project, proper documentation, testing, etc. Furthermore, a number of additional quality measures are essential in producing digital equipment for important applications in nuclear power plants.

For example, design reviews and independent assessments at various phases of the project are important steps that should be emphasized. The reviews could, depending on the part of the project being reviewed, be general in some cases and more specific and detailed in other cases.

Those in charge of preparing the QA plan for a digital I&C project should use their own discretion as to the extend of detail that is necessary for design reviews, independent assessments, etc.

As for other general requirements on work processes the following may be helpful:

(i) High Level Programming Languages. Although this practice is already very common, it is worth mentioning that high level programming language has proven to contribute to qualify of software and software based products.

(ii) Structured Programming Techniques. It is obvious that any software or software based equipment for any important application in a nuclear power plant should be developed using a structural programming approach. The software developer should have adequate formal training to write the software using software design criteria driven from the technical specification for the equipment.

(iii) Limited Use of Nested Loops. Any complex program normally includes nested loops. Although the use of nested loops does not have to be avoided; experience has shown that limiting the number of nested loops can contribute to increase software quality and reduce failures.

(iv) V&V of design modules. Upon completion of each major phase or module of a digital I&C design or implementation, a V&V effort may be warranted as this will help avoid later problems when the system is integrated. The extent of this effort should be established by the project technical group and endorsed by project QA group. Obviously, complete V&V of each module would be the best approach if this is warranted by the project scope, budget, and schedule. However, a more restricted testing of small modules may be possible, provided that enough confidence in its functionality can be placed to take the risk that final test of the integrated system will uncover problems, which may have escaped during earlier tests of individual modules.

Also, as was mentioned earlier, a separation between I&C system platform and the associated plant specific application software has proven to be a good practice. Furthermore, a software design strategy to include easy error detection and recovery in all phases of an I&C digital design and implementation is helpful for producing reliable digital equipment. It is a good practice to verify the quality of the output from each work process as early as possible to ensure that errors are not passed forward to later stages.

6. CONCLUSIONS AND RECOMMENDATIONS

I&C systems have an important position in ensuring the safety of nuclear power plants and therefore, convincing evidence that they will fulfill their intended function has to be produced during the licensing process. Important licensing issues have to be considered in the design and implementation process, such as the safety classification and other important guiding principles. A harmonization of the licensing requirements and later perhaps also the licensing process would facilitate a cost effective assessment of the quality of digital I&C. It

is believed that the present variety of national licensing approaches of digital I&C in the long run can have a negative impact both on safety and economy of nuclear power plants.

The nuclear industry has reached a point where it is no longer practical just to produce more documents on how to license digital I&C. The challenge now lies in reducing the documents to a set, which is structured and can give true support. Because there is a large diversity in national requirements for digital I&C, it is not likely that harmonization will be achieved on a short term. By a correct targeting of efforts it should, however, be possible to achieve a better harmonization in a longer term, but that implies an agreement on the technical and scientific requirements basis to be used in designing and licensing of digital I&C.

Presently national regulators have a practice, where international norms and standards are mentioned and referred to. The influence of international norms and standards is however relatively weak as compared to national requirements. A stronger reliance on international standards in the licensing process would in the long run make results of a specific licensing process reusable for other plants and in other countries. If that can be achieved there are several benefits to be obtained both with respect to the efforts in the licensing process and the safety of the nuclear power plant due to a balanced design of the I&C.

6.1. CONCLUSIONS

There is clearly a need for better harmonization of the licensing requirements of digital I&C. There are no technical nor scientific reasons for the present diversity in the requirements. If a harmonization cannot be advanced it will be difficult to find cost effective approaches to the licensing of digital I&C. This may leave the nuclear industry in a situation where it due to difficulties in the licensing process may consider it impossible to enter modernization's which clearly would improve the safety of the plants. This is not in the interest of anybody. A harmonization of licensing requirements may also make it easier for the nuclear industry to utilize the experience collected by the conventional industry in the field of safety important I&C.

The most important step in approaching a development towards harmonized licensing requirements for digital I&C is to create an understanding of its benefits. It is evident that harmonized licensing requirements have a potential of making it easier to share both experience and actual evidence on a global level that a certain system is practically free of error. If this can be achieved there is no doubt that an improved safety can be reached at the same time as costs and efforts of the licensing process can be kept on a moderate level. The difficulty seems to be to agree on the steps to be taken for generating specific evidence of functionality of the I&C and the depth into which this evidence should go.

Referring to increasing globalization of both nuclear utilities and I&C vendors, there have to be reasons that a system, which is considered acceptable in one country, cannot be accepted in another. Such reasons could be connected to the nuclear site itself or its environment, but just a reference to national requirements without putting them in perspective can only lead to a loss of trust and confidence by the public. Any approach towards better harmonized licensing requirements has to be built on agreed upon high level requirements and basic safety principles. Only if there is a traceable path between these and the more detailed requirements it is possible to compare systems of requirements and to put them into perspective.

Considering in general the experience from digital I&C it seems that the technology sometimes unfairly has been blamed for problems that have arisen not from the technology itself, but from unsatisfactory specifications or flawed engineering processes. In this light, it seems fair to conclude that prudent engineering practices and methods should leave very few undetected errors in the final products that are applied in safety related applications.

Considering the broad areas of safety I&C and safety-relevant I&C, there does not seem to be that large of a difference in opinion within the highest safety classes, but more in how these requirements should be relaxed in lower safety classes. This gives an indication of areas where more efforts may be needed. In some Member States the largest dispute regarding licensing requirements seems to be in the classes where it may be reasonable to use standard components from the conventional industry. Only if requirements are harmonized will it be possible to get a large enough experience base from the application of such components to arrive at believable reliability estimates for them.

A path towards harmonization can be reached only through identification of crucial steps in the confidence building process of digital I&C. By a reflection of how these are considered in national practices it should be possible to create a better understanding of how national practices differ and to make it possible to initiate a consensus building process.

Over the last decade, some licensing authorities have adopted risk informed regulation practices. These practices call for budgeting the regulatory attention based on the importance of the equipment being reviewed. This practice is certainly a sensible approach also for licensing of digital I&C equipment. However, due to the inherent properties of digital equipment, it is not always easy to formulate such risk-based reviews.

The classification system by which functions and systems are graded is a key to harmonization. The classification systems are anchored to general principles, which again are deduced from the higher level safety requirements. These principles are very important, because harmonization cannot be reached if there is no agreement on how these principles are interpreted. Unfortunately there seems to be a large variety between national approaches even on this fundamental level. Also the simple question of the number of classes to use in a classification system seems to stimulate vivid discussions. An in depth discussion on classification systems has to rely on general safety principles, but it seems also necessary to initiate a more generic discussion of their relationships with deterministic and probabilistic safety thinking in the design of nuclear power plants. The question here is to what extent deterministic requirements could be relaxed using probabilistic reasoning and vice versa. Another issue, which may warrant in-depth discussions, is the structure of requirement system itself. How should requirements be formulated and how should their relationships be indicated.

6.2. RECOMMENDATIONS

There is a clear need for better information exchange between those international bodies (IAEA, IEC, IEEE, etc.) with respect to ongoing and planned activities. It may even be a good idea to appoint a small expert group to develop a long term vision for how to reach an improved harmonization within design and licensing of digital I&C. A harmonization is expected to bring forward an increased reliance on international norms and standards. It can also be expected that the licensing requirements for I&C become more closely integrated in the more general licensing requirements for nuclear power plants.

Some important steps have already been taken towards an increased harmonization in licensing requirements in general. These include, but are not restricted to, the national responses to the Nuclear Safety Convention, utility cooperation in creating their own requirements and the regulators cooperating in various bodies. It is important that these activities are further encouraged.

In creating a path towards better harmonization it would be important to create a vision for future development of the I&C technology, not to come with too detailed requirements too early. It would also be necessary to plan for the highest possible reuse of earlier designs, not to introduce the burden of and danger in a redesign of earlier well-proven solutions.

In entering a path towards harmonized licensing requirements, it would be necessary to create a better understanding of variations in systems of requirements. To reach this end it would be necessary to compare important documents to see where they agree and where they differ. That can be achieved only if there is a well-documented relationship between higher level requirements and the detailed requirements set on the I&C. Only then it is possible to have an understanding of the reasons for the difference. If a generic model for I&C projects could be developed it could serve as an aid to structure concepts, actions and documents to be used in the licensing process. This model has to be created in a top down fashion from the structured requirements system. Such a model could also support the creation of a terminology to be used in the licensing of I&C systems for nuclear power plants.

Some of the issues within licensing of digital I&C seem to require a more in-depth discussion. One of these issues is the relationship between deterministic and probabilistic criteria. A safety function at a nuclear power plant is designed with a reliability target in mind and it is implemented with a certain process system, which for its function relies on the I&C. The question in this context is the principles for calculating backwards from a target reliability of the safety function to arrive at specific requirements for the I&C. Similarly deterministic design principles can be used to eliminate certain failure mechanisms within the digital I&C and then the question is what kind of credit these design principles can be given in a probabilistic sense.

Another issue which may warrant an in-depth discussion is the structure of requirement systems. Specific requirements are in reality often written as prescriptions with reference to certain solutions, instead of giving a requirement that can be verified with a reasonable effort. This question may also lead to a more generic discussion of the relative quality of different requirement systems. An in-depth discussion of these issues could lead to a better understanding of the confidence building process within the licensing of digital I&C. Harmonized licensing requirements have to be based on technical and scientific considerations. With the present level of understanding it is evident that there is a need for more research.

Harmonization can only be achieved if there is a strategy towards increasingly applying international standards in national licensing processes. It has to be born in mind that these standards are based upon a broad consensus on the engineering issues when assessing nuclear safety and therefore have the ability to provide a solid basis for mutual understanding and enhance harmonization. In this context IEC SC45A standards are examples; especially the standards on classification and requirements for I&C systems important to safety and safety critical software gain considerable acceptance in many countries. In the area of digital I&C which presumable still rapid development it would therefore technically and economically more efficient to put the efforts in the development of international standards than to duplicate this work at a national basis.

Whenever the norms and standards for understandability purposes are translated to another language it seems to be a sound strategy to maintain only the original as binding and to treat all translations as to be created for information only. If a harmonization is achieved, there is a prospect also of making the results of a specific licensing process reusable for other plants and countries. Then there are several benefits to be obtained both with respect to the cost of the licensing process and the safety of the nuclear power plant due to a balanced design of the I&C.

BIBLIOGRAPHY

Health and Safety Executive, four party regulatory consensus report on the safety case for computer-based systems in nuclear power plants, produced by AECB-Canada, DSIN/IPSN – France, NII – UK, USNRC – USA, November 1997.

European Commission – Nuclear safety and the environment, Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors, EUR-19625, May 2000.

IAEA SAFETY STANDARDS SERIES, DS 252, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, August 2000.

INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants – Instrumentation and control systems important to safety – Categorization of safety functions, Standard No. 61226, Geneva, 1993.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Standard 603, 1991.

INTERNATIONAL ATOMIC ENERGY AGENCY, Specification of Requirements for Upgrades Using Digital Instrument and Control Systems, IAEA-TECDOC-1066, January 1999.

INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems, Standard No. 61513, Geneva, 2001.

INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software, Standard No. 60880-2, Geneva, 2000.

INTERNATIONAL ATOMIC ENERGY AGENCY, Effective Handling of Software Anomalies in Computer Based Systems at Nuclear Power Plants, IAEA-TECDOC-1140, March 2000.

INTERNATIONAL ATOMIC ENERGY AGENCY, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, IAEA-TRS-384, 1999.

DEFINITIONS

The following definitions are used for concepts and terms used in this publication.

Code	In software engineering, computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler or other translator [IEEE 610.12-1990].
Common Cause Failure (CCF)	Common cause failure. The failure of a number of devices or components to perform their functions as a result of a single specific event or cause (IEC 61513). The event or cause which triggers the I&C system failure may be internal or external to the safety system, a specific process dependent loading, a human induced operation or a maintenance error, a natural phenomena or a change in ambient conditions.
Complexity	(1) The degree to which a system or component has a design or implementation that is difficult to understand and verify. (2) Pertaining to any of a set of structure-based metrics that measures the attribute in (1). [IEEE-610.12-1990].
Component	One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components. [IEEE-610.12-1990].
Defense in Depth	Concept which provides a major contribution to the safety philosophy. DiD has to be applied to all safety activities, whether organizational, behavioral or design-related, to ensure that there are overlapping safety provisions so that if a failure does occur, it would be compensated for or corrected (IAEA 50-SG-D8).
Deterministic design requirements	In the deterministic approach, design basis events are chosen to bound a range of related possible initiating events which could lead to a challenge to the safety of the plant (A.2.2 of IEC 61513).
Diversity	Existence of two or more different ways or means of achieving a specific objective. Diversity is specially provided as a defense against CCF. It may be achieved by providing systems that are physically different from each \other, or by functional diversity, where similar systems achieve the specific objective in different ways (IEC 61513).
Error	(1) The difference between a computed observed or measured value or condition and the true specified or theoretically correct value or condition (2) An incorrect step, process or data definition. (3) An incorrect result (4) A human action or process that produces an unintended result. [IEEE-610.12-1990].
Failure	The inability of a system or component to perform its required functions within specified performance requirements. [IEEE-610.12-1990].
Fault	(1) A defect in a hardware device or component. (2) An incorrect step, process or data definition in a computer program. [IEEE-610.12-1990].

Function	(1) A defined objective or characteristic action of a system or component. (2) A software module that performs a specific action is invoked by the appearance of its name in an expression, may receive input values, and return a single value. [IEEE-610.12-1990].
Formal specifications	Specifications that have been written using a formal language.
Hardware	Physical equipment used to process, store or transmit computer programs or data. [IEEE-610.12-1990].
Harmonization	The process of making two or more sets of requirement systems or work processes more similar to each other. The goal in the harmonization is also to build a better understanding for differences in the requirements or the work processes and their reasons.
I&C function	Function to control, operate and/or monitor a defined part of the process (IEC 61513).
I&C system	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 system itself. The term is used as a general term which encompasses all elements of a system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices (IEC 61513).
Licensing process	The work process to generate and document evidence that certain solutions is acceptable from a safety point of view.
Licensing requirements	The requirements to which certain technical solutions are compared to decide on their acceptability during the licensing process.
Performance	The effectiveness with which a function is carried out (e.g. time response, accuracy, sensitivity to parameter changes).
Postulated initiating event (PIE)	PIEs identify events that lead to anticipated operational occurrences or accident conditions and their consequential failure effects (IEC 61513).
Probabilistic requirements	Requirements set for instance on the reliability of functions, components or systems at predefined integration levels.
Protection system	System, which monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.
Quality Assurance	All those planned and systematic actions necessary to provide adequate confidence that an item (component, function or system) or service will satisfy given requirements for quality [IAEA Safety Series No. 50-C-QA (rev.1)].

Quality system	A described way to reach a defined and acceptable quality in work processes that are important for safety (cf. Quality Assurance).
Redundancy	Provision of alternative (identical or diverse) elements or systems, so that any one can perform the required function regardless of the state of operation or failure of any other [IAEA Safety Guide No. NS-G-1.1 Software for computer based systems important to safety in nuclear power plants].
Reliability	Probability, that a device, system or facility will perform its intended functions satisfactorily for a specified time under stated operating conditions (IAEA 50 SG-D8).
Requirement	(1) A condition or capability needed by a user to solve a problem or achieve an objective. (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents. (3) A documented representation of a condition or capability. [IEEE-610.12-1990].
Response Time	The elapsed time between the end of an inquiry or command to an interactive computer system and the beginning of the systems response. [IEEE-610.12-1990]
Response Time Testing	Measurements to identify the response time.
Safety	The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of site personnel, the public and the environment from undue radiation hazards.
Reusable software	Software module that can be used in more than one computer program or computer system (IEC 61513)
Safety Action	A single action taken by a safety actuation system.
Safety Actuation System	The collection of equipment required to accomplish the required safety actions when initiated by the protection system.
Safety Function	A specific purpose that must be accomplished for safety. [IAEA Safety Standards Series No. NS-R-1, Safety of nuclear power plants: Design]
Safety Systems	Systems important to safety, provided to ensure, in any condition, the safe shutdown of the reactor or the residual heat removal from the core, and/or to limit the consequences of anticipated operational occurrences and accident conditions [IAEA 50-SG-D8].
Single failure	Random failure which results in the loss of capability of a component or system to perform its intended functions. Consequential failures resulting from a single random occurrence are considered to be part of the single failure (IEC 61513).

Single Failure Criterion	Assembly of equipment, which satisfies the single failure criterion if it is able to meet its purpose despite a single random failure, assumed to occur anywhere in the assembly. Consequential failures resulting from the assumed single failure are considered to be an integral part of the single failure (IEC 61513).
Software	Computer programs, procedures and possibly associated documentation and data pertaining to the operation of a computer system. [IEEE-610.12-1990]
Software Life Cycle	The period of time that begins when a software product is conceived and ends when the software is no longer available for use. The software life cycle typically includes a concept phase, requirements phase, design phase, implementation phase, test phase, installation and validation phase, operation and maintenance phase and sometimes, retirement phase. [IEEE-610.12-1990]
System	A collection of components organized to accomplish a specific function or set of functions. [IEEE-610.12-1990]
I&C upgrade	To design, provide and install equipment to replace equipment, hardware and software of one or more systems, with added functionality, performance or reliability features. An example would be to provide a new information, display and logging computer system, with VDU displays and logs, replacing analogue control room instruments and a rector monitoring computer. Another example would be to replace a control room array of alarm annunciators with a computer-based system with automatic logic to assign safety or operational importance to each alarm.
Validation	The testing and evaluation of the integrated computer system (hardware and software) to ensure compliance with functional, performance and interface requirements. [IEC 880]
Verification	The process of determining whether or not the product of each phase of the digital computer system development process fulfils all the requirements imposed by the previous phase. [IEC 880]

ABBREVIATIONS

The terms that are commonly used in the subject areas of digital I&C are summarized below. The abbreviation for each term is identified in the table followed by a description of the term.

ALARA	As Low As Reasonable Achievable.
BBN	Bayesian Belief Networks
CCF	Common cause failure.
COTS	Commercial Off The Shelf, a standard industrial grade components from which it is practically impossible to get information on how they were designed
CPU	Central Processing Unit
DBA	design basis accident, an accident sequence, which provides the basis for the design of safety systems
EMC	Electromagnetic compatibility.
EMI	Electromagnetic interference. See EMC.
EMI / RFI	Electromagnetic Interference / Radio-Frequency Interference. Environmental conditions which can affect the operation of digital equipment.
ESD	Electrostatic Discharge
EUR	European Utilities Requirements
FAT	Factory Acceptance Test
FMEA	Failure Mode Effects Analysis
FSE	Functions, systems and equipment
HMI	Human Machine Interface
I&C	Instrumentation and control, concept encompassing all functions by which automatic and manual control actions are initiated, logged, and signaled
MMI	Man-machine interface. See HMI.
NSR	Non safety-related
PIE	Postulated Initiating Event
QA	Quality Assurance
SAR	Safety Analysis Report
SAT	Site Acceptance Test
SFC	Single failure criterion
V&V	Verification and validation

APPENDICES A

APPENDIX A.1.

BELGIUM, COUNTRY REPORT
(provided by J.-C. Naisse, Tractebel)

Belgian NPPs: Background and actual approach for classification of digital I&C systems and associated hardware/software requirement gradation

1. SITUATION DURING CONSTRUCTION OF THE FOUR LATEST BELGIAN NPPS

The four latest Belgian NPPs (Doel 3, 4 and Tihange 2, 3 – 1000 MW(e) PWRs) were ordered around 1975 and commissioned in between 1982 and 1985.

For design, erection, commissioning and operation of those plants the regulatory framework adopted was constituted by the Belgian legal framework with integration of (or comparison to) the rules published by the USAEC and the NRC.

Considered US rules were General Design Criteria of 10 CFR Part 50, the Regulatory Guides, the IEEE Standards, the ASME code, … in their versions as available in July 1974.

In the design stage of the plants an extensive interpretation of those US rules was performed in order to determine the I&C and Electrical systems/equipment that had to be classified 1E. Those equipment/system were selected among the "protection systems" according IEEE 279, the "systems important to Safety" according 10CFR50 Appendix A, the "safety systems" according IEEE 603. At that time digital I&C systems were implemented only for non 1E purposes: Computerised Information System, Steam Generator Level Control System, Turbine Steam Dump Control System, …

As a consequence, only analog I&C systems/equipment were to be found as 1E classified and associated qualification methodologies and programmes were developed according IEEE 323. Three sub-categories (1EA, 1EB and 1EC) were considered requiring respectively qualification to in-containment LOCA conditions, to harsh outside containment conditions and to mild environment.

2. EVOLUTION OF THE SITUATION FOR HARDWARE CLASSIFICATION/QUALIFICATION

Above adopted binary 1E/non 1E splitting led to 1E classification (and according qualification) of a large number of I&C equipment/systems in addition to those purely related to the "protection systems".

Hardware classification aspects

First years of operation of the plants showed very rapidly that this was putting an important burden to the Utility as far as periodic testing required by Technical Specifications was concerned.

It was recognised necessary to consider for the 1E equipment/systems:

- relaxed or additional design criteria in case of replacement,
- the capability and procedures for periodic testing and calibration,
- the extension of the Technical Specifications in the field of surveillance requirements, limiting conditions for operation.

A review was carried out by the Utility, its Architect Engineer and the Safety Authorities to review for each Belgian NPP the safety significance of all I&C equipment/systems classified as 1E. This work was performed first for the four latest plants and extended afterwards to the first Belgian NPPs of Doel 1&2 and Tihange 1 (commissioned in 1974/75).

A splitting of the I&C equipment/systems of class 1E into three categories (1E1, 1E2 and 1E3) was chosen – inspired from considerations provided in IAEA Safety Guide 50-SG-D8 "Safety Related I&C systems for NPPs" and from the categories used in the RG 1.97 for the Post Accident Monitoring System. Those three sub-categories showed to allow for sufficient gradation in the safety roles and in the sets of criteria/requirements while leading to a classification system easy to use both during design and during operation. In addition it appeared to be almost compatible with A, B and partly C categories as defined afterwards in IEC 61226 standard.

Safety Analysis Reports of the plants were adapted to take above classification into account.

Hardware qualification aspects

First I&C equipment/system replacement that occurred in the frame of the 1EA/1EB/1EC sub-categories indicated also the possible benefits that could be driven from adopting a more graduated qualification approach.

Five levels were defined:

- 1EA as before but in turn taking into account the time after accident the equipment/system had to retain its functionalities — (very) short term/medium term/long term,
- 1EB as before but distinguishing location with or without radiation exposure,
- 1EC as before — off-process with mild controlled environmental conditions,
- 1ED on the process but in mild controlled environment with negligible radiation,
- SIS where only earthquake and vibration resistance is to be considered.

This five level categorisation and the associated requirements (as far as environment, ElectroMagnetic Compatibility, ageing, earthquake, radiation exposure, Loss Of Coolant Accident conditions, post-accident ageing) are concerned are of common use presently for each new required I&C equipment/system qualification.

3. APPROACH ADOPTED FOR CLASSIFICATION/QUALIFICATION OF DIGITAL I&C SYSTEMS

First implementation of digital I&C systems in 1E applications occurred in 1990 along with adjunction of Ultimate Emergency Systems to the Doel 1&2 plants. Hardware qualification occurred according the methodology outlined in section 2 here above. For software

qualification the US regulatory framework was again taken as a reference and RG 1.152 – IEEE 7.4.3.2 were taken into account.

During licensing of the systems the Safety Authorities referenced however the IEC 60880 which led to some extra software verification work (reverse engineering verification of actuator control logics, internal variables crosschecks for the protection system software, additional basis software audits at the manufacturers)

Further problems encountered up to the mid-nineties with licensing of digital I&C systems in the Tihange and Doel units (sub-cooling margin and critical functions monitoring system, 6kV protection relays, PAMS recorders, Radiomonitoring measurements) showed that a global re-assessment of the classification/qualification methodology (mainly as far as software was concerned) was a must in order to allow for further possible implementation of such systems.

Discussions started end 1996 between the Utility, its Architect Engineer and the Belgian Safety Authorities in order to define a practical approach for software classification/qualification.

Software classification aspects

Main prerequisites/concerns were:

- to cope as much as possible with the A, B, C classification as given by IEC 61226 standard
- to remain in coherence with the already determined Function-System-Equipment classification in 1E1/1E2/1E3 sub-categories as written down in the plant's SARs

This came out in a five fold classification according the I/II/III sub-categories for software of 1E classified FSE and the IV /V(N) sub-categories for software of non 1E classified FSE.

The two first sub-classes I/II are matching the 1E1/1E2 sub-classes of SAR and A/B classes of IEC 61226. Sub-class III matches 1E3 but is a sub-set of IEC 61226 class C which covers also sub-class IV. Sub-class IV stands for FSE that were considered non 1E at the construction of the plants but which are however to be considered as linked to safety.

Software qualification aspects

Relying on the above classification a gradation in the software quality/qualification requirements was worked out for the aspects related to:

- applicable norms and standards
- quality assurance
- design
- verification & validation
- documentation
- return of experience

For software of sub-class I requirements of IEC 60880 apply in full. For sub-class II and III gradual relaxations were defined for each above listed aspects. Requirements for sub-class IV are matching those of sub-class III, difference here is about the licensing process and the involvment of the Safety Authorities.

4. CONCLUSION

The classification of HardWare and SoftWare of digital I&C equipment/systems as used in Belgium can be summarised according the table given in appendix. A logic diagram was developed to provide a tool to help determining needed classification of FSEs.

The graduated requirements for the different aspects of SoftWare qualification for 1E digital I&C equipment/systems has been summarised in a consensus document which allows for licensing discussions based on a common understanding of the requirements.

The consensus that was reached in Belgium for classification/qualification of HardWare and SoftWare for digital I&C systems allowed in the last three years for smooth and successful implementation of important I&C modifications in the Belgian NPPs of the Doel and Tihange sites (Radiation monitoring, Ex-Core Neutron Instrumentation System, Thermodynamical Instrumentation System).

Appendix

Classification of FSE

<table>
<tr><th>SAR</th><th>Hardware</th><th>Software</th><th colspan="3">Functions-Systems-Equipments</th><th>IEC 61226</th></tr>
<tr><td>1E1</td><td>1E</td><td>I</td><td colspan="2">Protection systems</td><td rowspan="2">Important to safety</td><td>A</td></tr>
<tr><td>1E2</td><td>1E</td><td>II</td><td rowspan="2">Direct impact on safety</td><td rowspan="3">Other safety systems</td><td>B</td></tr>
<tr><td>1E3</td><td>1E</td><td>III</td><td>Related to safety</td><td rowspan="2">C</td></tr>
<tr><td>N1E</td><td>N1E</td><td>IV</td><td>Indirect impact on safety</td><td>Linked to safety</td></tr>
<tr><td>N1E</td><td>N1E</td><td>V(N)</td><td colspan="3">Non important to safety</td><td>N</td></tr>
</table>

APPENDIX A.2.

CZECH REPUBLIC, COUNTRY REPORT
(provided by C. Karpeta)

Current Regulatory Practice and Industry Standards in Czech Republic

1. REGULATORY ENVIRONMENT FOR THE REFURBISHMENT OF NPP I&C SYSTEMS

Czech Republic legislation which governs the safety aspects of siting, design, construction, commissioning, operation and decommissioning of nuclear installations can be viewed as structured into the following two level hierarchy:

- acts passed by the Parliament
- regulations issued by the State Office for Nuclear Safety (SONS).

The upper level legislation which addresses the above mentioned aspects is the Act on Peaceful Utilisation of Nuclear Energy and Ionizing Radiation (Act No. 18/1997 Coll., i.e. the so-called Atomic Act). This Act regulates various areas connected with the uses of nuclear power and ionizing radiation. Its provisions which specifically apply to the implementation of changes affecting nuclear safety, radiation protection, security and emergency preparedness of nuclear installations, hence also to the refurbishment of the I&C systems important to safety, are those that:

- define the powers and responsibilities of the State Office for Nuclear Safety
- set forth general and specific conditions for performing activities associated with the uses of nuclear power
- cover handling of radioactive wastes
- define the contents of the documentation that has to be submitted to the SONS as the documentation accompanying the nuclear facility operator's application for the permission (license) to implement changes affecting nuclear safety.

The lower level legislation, which is most relevant to the I&C systems of nuclear facilities, is the following group of the SONS regulations:

Regulation No. 195/1999 Coll. on the requirements for the assurance of nuclear safety, radiation protection and emergency preparedness in nuclear installations

Regulation No. 214/1997 Coll. on quality assurance in activities relating to the uses of nuclear power and activities having a potential for causing irradiation and on specification of criteria for assignment of the selected equipment to safety classes

Regulation No. 106/1998 Coll. on the assurance of nuclear safety and radiation protection in commissioning and operation of nuclear installations.

Regulation No. 195 sets requirements pertinent to the design of systems important to safety. These requirements are of rather general nature comparable e.g. to the US NRC General Design Criteria. The provisions of this regulation which address the design for safety

of the plant I&C systems provide functional and design requirements covering the following areas:

- defense-in-depth,
- quality assurance,
- protection against equipment failures,
- fire protection,
- protection against the effects of natural events,
- protection against events caused by human activities outside the nuclear installation,
- plant instrumentation and control systems,
- plant protection systems,
- relations between the plant protection and instrumentation and control systems,
- plant control points,
- systems for reactor shutdown,
- power supply systems.

Regulation No. 214 deals in detail with quality assurance aspects of the activities associated with siting, design, construction, commissioning, operation and decommissioning of nuclear installations. It covers the following topics:

- implementation of the quality assurance system
- quality assurance system requirements
- requirements for quality assurance of the selected equipment with regard to its ranking into safety classes
- requirements pertinent to the scope of the quality assurance programs
- criteria for the assignment of the selected equipment to safety classes
- the format and contents of the list of the selected equipment.

Regulation No. 106 addresses those aspects of safety assurance, which are relevant to the commissioning and operation of nuclear installations including startup of nuclear power plants after refuelling. It specifies:

- general requirements for the commissioning and operation of nuclear installations
- technical and organizational conditions of safe commissioning of nuclear installations which cover, in particular:
  - the specification of the individual stages of the nuclear installation commissioning
  - the specification of documentation to be submitted to the regulatory authority for evaluation in the process of issuing permissions to begin and proceed through the individual stages of the commissioning
  - limits and conditions of safe operation of a nuclear installation (technical specifications)
  - technical and organizational conditions of safe operation of nuclear installations
  - requirements to be met when reaching reactor criticality after refuelling.

Industry standards which address various aspects of the design for safety of the NPP I&C systems are the IEC and EN standards that have been accepted as national standards, i.e. the CSN standards.

2. REGULATORY REQUIREMENTS SET FORTH FOR THE NPP DUKOVANY I&C REFURBISHMENT PROJECT

NPP Dukovany is a four-unit VVER-440 plant that was designed in mid-seventies and has been in operation since 1985. A contract for a large scale I&C refurbishment project was concluded in the year 2000 between CEZ, i.e. the utility operating this plant, and a group of vendors including ŠKODA Nuclear Engineering as the main contractor and FRAMATOME, SCHNEIDER ELECTRIC, ZAT Příbram and I&C ENERGO companies as subcontractors, for the design and implementation of digital computer based I&C portions of the plant safety systems and some safety-related systems. Two groups of regulatory requirements apply to this project.

In the first place, SONS set in its Resolution No.79/1999 the requirements concerning the scope of the I&C refurbishment project (the following I&C systems have been required to be modernized: reactor trip system, engineered safety features actuation system, diesel sequencer system and the reactor power limitation system), and general requirements for ensuring functionality, reliability, performance, equipment qualification and quality assurance of those systems in line with the applicable provisions of the Czech legislation, i.e. the regulations No.195, 214, and 106. These requirements were included in the call for bids as a part of the specifications of the I&C systems to be modernized (i.e. not only those requested by SONS) and have been considered during the conceptual design and the basic design of the refurbished systems or will be considered at a later time during the project implementation as follows:

- compliance with the Regulation No.195 was focused upon in establishing the design basis and system requirements both for the innovated plant I&C system as a whole, as well as for the I&C portions of the individual plant safety and safety-related systems;
- the I&C refurbishment project overall quality assurance plan was established in line with the requirements of the Regulation No.214 pertinent to such entities as processes, activities, products, organizations, personnel, and their combinations; more specifically, the provisions of the article 23 of this regulation which apply to the so-called “specific processes”, i.e. processes the results of which cannot be fully verified through checking and testing, have been used as a regulatory basis for setting requirements to be met by the software development process of the safety critical software to be implemented in the refurbished I&C systems built on programmable digital platforms; quality assurance systems of all the contractors participating in the refurbishment of the I&C systems important to safety will have to be compliant with the applicable provisions of this regulation;
- conformance to the applicable provisions of the Regulation No.106 will be the subject of those I&C refurbishment project activities that relate to updating of the existing plant technical specifications and operational procedures during and after completion of the innovated I&C systems implementation, and to testing of the installed new I&C systems prior to the plant startup after completion of the individual stages of the I&C system refurbishment during the plant planned outages.

In the second place, SONS set in its position paper dated August 2000 the following series of specific requirements pertinent to some aspects of the refurbishment project:

Classification of the I&C systems important to safety

Safety classification of the I&C systems important to safety shall be performed on a deterministic basis in compliance with the guidance given in the IEC Std. 61226, i.e. assignment of the I&C functions and the associated systems and equipment to the following categories: category A, B, and C.

Acceptability of the digital computer-based I&C systems important to safety

Implementation of the refurbished I&C systems important to safety using software based digital computer technology is acceptable provided that:

- the design, manufacturing, installation, testing, commissioning and operation of those systems will meet all the applicable provisions of the Czech legislation
- those systems will meet all the requirements stated in the SONS resolution No. 79/1999
- those systems will meet the specific requirements stated under the next headings
- those systems will meet, to the extent reasonably achievable, the requirements and recommendations of the applicable IAEA documents, IEC standards, national industrial standards such as the CSN and IEEE standards, and the US NRC General Design Criteria and Regulatory Guides.

Special attention will be paid during the licensing assessment to the evaluation of the conformance to these requirements.

Software development process for the I&C systems important to safety

Software development process for category A I&C functions shall be a well-structured process consisting of the following activity groups:

- planning activities
- development activities, i.e. requirements activities, design activities, implementation activities, validation activities, and installation activities
- integral activities, i.e. verification activities, configuration management activities, and safety analysis activities.

Software development process for category B I&C functions shall be basically the same as the one for category A functions.

Software development process for category C I&C functions shall be the same as that for high quality industrial I&C applications.

Verification and validation of the software for the I&C safety systems

For the software implementing category A I&C functions the following shall apply:

- V&V activities compliant with the requirements of the IEC Std. 880 and NRC RG 1.152 shall be performed during the software development process as well as during the consecutive life-cycle phases

- no third party independent V&V activities are required provided that the software V&V team at the manufacturer is management and financial independent of the development team
- audits of the software development process shall be performed right from the startup of this process.

Defence against common cause failures (CCF) in the software of safety systems

With respect to the postulation of CCF the following shall apply:

- CCFs will not need to be postulated in safety system hardware including the sensors
- CCFs will have to be postulated in complex software implementing safety functions
- CCFs will not need to be postulated in simple software modules participating in implementation of safety functions provided that:
  - these software modules can be fully tested, or
  - extensive positive operational experience from previous applications in similar safety applications is available and well documented
  - CCFs will not need to be postulated in software modules implementing support functions such as e.g. software for on-line diagnostics provided that it can be proved that errors in this software cannot degrade performance of the safety functions.

Implementation of diverse means of protection against the postulated CCFs:

- is required with respect to the ANSI Condition II and III plant design basis events (postulated initiating events) with the estimated frequency of occurrence greater than 10E-3 per year
- is not required for less frequent plant design basis events, i.e. for some ANSI Condition III events and all ANSI Condition IV events.

The following relaxed acceptance criteria can be applied in the accident analysis of the safety actions initiated by the diverse means of protection:

- maintenance of coolable core geometry
- maintenance of the primary coolant system integrity
- maintenance of the hermetic zone integrity
- availability of sufficient time (not less than 30 minutes) for taking manual safety actions as the diverse means of protection.

The following two approaches in diversity implementation will be viewed as adequate:

- functional diversity implemented in two functionally isolated subsystems of a safety system which process two different groups of input signals, or
- implementation of a separate diverse protection system which features functional isolation of the primary protection system, different hardware and different software.

Adequacy of the diversity implementation shall be supported by analysis.

Communications between subsystems of the digital computer-based I&C safety systems

Requirements set forth on the communications between subsystems of the I&C safety systems are as follows:

- no failure in a subsystem of a safety system division shall affect the performance of safety functions in the redundant divisions of this system.
- sharing of data among the redundant divisions of a safety system, including sharing of input signals, shall not degrade the functional isolation of those divisions.
- loss of communication between redundant divisions shall not cause interruption of the division activities.
- all communication links shall be checked by on-line diagnostics.
- the fail-safe design principle shall be applied where practically achievable to provide for pre-defined reaction of a safety system to the loss or degradation of the communications.

Testability of the digital computer-based I&C safety systems during reactor operation

- the on-line diagnostics shall perform three functions:
  - upon system startup and re-starts it shall check the status and the correctness of hardware functioning and the configuration of the installed software
  - during system operation it shall check sequentially in each code execution cycle the status and correctness of hardware functioning in such a way that the full-scope checking be completed in about 10 minutes
  - during system operation checking of the communications based on the diagnostic information contained in the messages transmitted over the communication links and supported to the maximum possible extent by implementation of Deadman Timers which indicate interrupts in the communications

- periodic surveillance testing shall provide for:
  - testing of the hardware of the system command features that participate in performing the safety and on-line diagnostic functions and is not tested by the system on-line diagnostics
  - if there are no hardware components covered by the system on-line diagnostics then the periodic surveillance testing need not to be implemented

- the provisions of §18 section (1) of the SONS regulation No.195/1999 Coll. must be met during system testing, i.e. the single failure criterion and the minimum redundancy requirement.

Compliance to the single failure criterion

The requirement for compliance of the I&C safety systems with the single failure criterion is stated from two perspectives:

- what concerns the type of single failures, the effects of the plant design basis events on the safety systems, and the impacts of a single failure occurrence the provisions of the IEEE Std. 379 are required to be met.

- what concerns the impacts of a single failure occurrence the provisions of the §18 section (1b) of the SONS regulation No. 195/1999 Coll. are also invoked to comply with the minimum redundancy requirement.

Exemptions from the conformance to the single failure criterion under extraordinary situations could be considered by the regulatory body on a case-by-case basis; this, however, does not apply to regularly occurring situations such as periodic surveillance testing. Separate diverse protection systems if implemented within the I&C system refurbishment project are not required to meet the single failure criterion.

Equipment qualification

An equipment qualification program shall be established for the refurbished I&C systems important to safety encompassing the following activities:

- program preparation
- equipment qualification implementation
- maintenance of the equipment qualification.

Program preparation activities should include specification of:

- the equipment to be qualified
- the functions to be performed by this equipment and the time interval during which the functions are required
- the equipment location in the plant
- the environmental and operational conditions of the equipment
- methods and procedures for performing the qualification.

Equipment qualification implementation activities should include one or a combination of the following: qualification by type testing as the preferred qualification method, qualification by analysis, qualification based on operational experience.

Qualification maintenance activities should include: preventive maintenance, procurement and stock of spares, monitoring of the environmental and operational conditions, tracing of failures, personnel training, etc.

Acceptance of qualification certificates will be governed by the applicable provisions of the Act No.22/1997 Coll.

Reliability

It is required that:

- numerical values of the quantitative reliability indicators be established for the individual I&C systems important to safety
- in setting those values for the safety systems the plant safety goal represented by the calculated core melt frequency of 10E-4/year shall be considered; for the other systems those values should be derived from operational considerations

- as a minimum set of the reliability indicators the instantaneous or average system availability and the frequency of spurious initiations shall be used
- qualitative reliability analyses shall be performed for all safety category A and B I&C systems employing the FMEA methodology or its FBA version for the digital computer-based systems
- quantitative reliability analyses shall be performed for all I&C systems important to safety using the FTA method; in these analyses the potential for CCF and human errors shall be considered, as appropriate.

The requirements discussed above have been derived from the applicable provisions of:

- the Czech Republic legislation
- the IAEA Safety Series documents and Technical Reports
- the IEC standards
- the US NRC Regulatory Guides and NUREGs
- national standards such as CSN and IEEE standards.

3. LICENSING PROCESS OF THE NPP DUKOVANY I&C REFURBISHMENT PROJECT

As per the provisions of the Atomic Act, reconstruction or implementation of other changes in nuclear installations that affect nuclear safety, radiation protection, emergency preparedness and physical protection (security) fall into the category of activities for which a license issued by the SONS is needed. The Act also outlines the contents of the documentation that must be submitted to the SONS in support of the application for such a license. The documentation shall include the following information:

- description and justification of the planned reconstruction or other changes
- updating of the documentation that was approved by the regulatory authority for the nuclear installation commissioning and operation
- anticipated time schedules for the implementation of the planned reconstruction or other changes
- evidence that the reconstruction or other changes will not adversely affect nuclear safety, radiation protection, emergency preparedness and physical protection of the nuclear installation.

Documentation quoted in the second bullet will have to be approved by the SONS. It includes, among others, the limits and conditions of safe operation (plant technical specifications – Tech Specs) and the list of the selected equipment.

The “one-step” licensing process to be applied for implementation of reconstruction or other changes that affect nuclear safety, radiation protection, emergency preparedness and physical protection of nuclear installations, as stipulated by the provisions of §9, (1), f) of the Atomic Act, was felt to be not quite adequate for the NPP Dukovany large scope several-stage I&C system refurbishment project. Therefore, a project specific licensing process has been conceived in several rounds of discussions between the plant operator and the regulatory body. This process is copying to certain extent the licensing process applied to new nuclear power plant projects.

More specifically, the licensing process to be applied in the refurbishment of the NPP Dukovany I&C systems important to safety, is structured as follows:

Stage 1

The objective of this stage was to obtain the regulatory body position on the concept of the refurbishment project based on the evaluation by SONS of the general technical and implementation aspects of the project. This stage was broken down into two phases:

Phase 1A

The safety case of this phase was based on the information generated by the conceptual design of the refurbishment. The following topics were addressed in the documentation submitted to SONS for assessment:

- description and justification of the plant I&C system refurbishment project
- description of the plant I&C system after completion of the refurbishment project
- preliminary discussion of the plant Tech Specs changes
- draft attachment to the list of the selected equipment
- preliminary time schedules of the refurbishment project implementation
- evidence on meeting the applicable requirements for ensuring nuclear safety at the level of detail corresponding to the outputs from the conceptual design.

Phase 1B

The safety case of this phase was based on the information generated by the next stage of the conceptual design that is referred to as the preliminary design. The topics addressed in the documentation submitted to SONS for assessment were the same as those of the phase 1A but the level of detail was reflecting the evolvement of knowledge resulting from the next stage of the design. Main focus of the phase 1B safety case was on the conservative safety analyses results to support the intended implementation of some new and modified functions of the reactor trip system and the engineered safety features actuation system.

Both the conceptual design and the preliminary design as well as the safety case documentation were worked out by the Czech design company Energoprojekt and reviewed by the project team members and their consultants. Some outputs of these efforts were also used in preparation of the documentation that was passed on to the bidders for the refurbishment project implementation.

Stage 2

The objective of this stage is to obtain, as per the provisions of §9(1)f) of the Atomic Act, the license to implement the refurbishment of the plant I&C systems important to safety. The safety case of this stage will be based on the results of the basic design of the refurbished I&C systems important to safety performed by the supplier contracted for the implementation of the I&C refurbishment project and by its subcontractors. The documentation to be submitted to the SONS for licensing assessment will consist of:

- a series of Topical Reports covering the following subject areas:
  - software life cycle planning (software development plan, software quality assurance plan, software verification and validation plan, software configuration management plan, software safety analysis plan)
  - equipment qualification (description of methodologies to be used in the environmental, seismic and electromagnetic compatibility qualification)
  - system reliability (description of methodologies to be used in qualitative and quantitative reliability analysis of the individual I&C systems)
  - design of the individual I&C systems
- supplement to the existing Final Safety Analysis Report (evidence that the applicable requirements of the design for safety have been met will be provided here to document that the refurbishment will not impair the nuclear safety of the plant)
- update of the limits and conditions of the plant safe operation
- draft attachment to the list of the selected equipment
- time schedules of the project implementation.

Stage 3

This stage will be broken down into two phases.

Phase 3A

The objective of this phase is to obtain the regulatory body position on the implementation aspects of the refurbishment project in each individual unit of the plant. The safety case will be a kind of an update of the stage 2 safety case based on the results of the detail design of the refurbished I&C systems for each unit. It will also include plans for installation, testing and commissioning of the refurbished I&C systems during individual implementation phases of the project at the subject plant unit. Positive position will provide the plant operator with a sound basis for giving its consent to the commencement of manufacturing of the I&C equipment.

Phase 3B

This phase is aimed at obtaining the regulatory body consent to the implementation of a specific part of the refurbishment which is to be accomplished during a particular planned outage for refuelling. Hence, it will be repeated as many times as is the number of outages necessary for the completion of the refurbishment at this unit. The safety case will again be a kind of an update of the previous phase safety case, i.e. either the 3A phase or 3B phase, and will in addition include:

- description of the initial and final state of the unit I&C system with respect to the actual phase of the refurbishment implementation
- installation, testing and commissioning plans specific to the actual implementation phase
- updates of the Tech Specs and of the list of the selected equipment specific to the actual implementation phase

- reports on the results of the equipment qualification and system verification and validation activities performed at the manufacturer on the systems to be installed during the actual implementation phase
- evaluation of the quality assurance plan fulfillment during manufacturing of the equipment to be implemented during the actual implementation phase.

Stage 4

The objective of this stage is to obtain the SONS permission for the reactor startup after refuelling as per the provisions of §9(1)e) of the Atomic Act, which at the same time will include the SONS consent to the operation of the refurbished I&C systems important to safety implemented during the current implementation phase. Hence, this phase will also be repeated as many times as is the number of outages necessary for the completion of the refurbishment at the subject plant unit. The safety case will again be a kind of an update of the preceding phase 3B safety case, and will in addition include:

- description of the actual state of the plant I&C system after completion of the current implementation phase
- evidence of the equipment and personnel readiness for operation (this will include the evaluation of the refurbished I&C system installation and pre-operational tests)
- update of the Tech Specs (if necessary).

After the completion of the last refurbishment implementation phase at a particular unit, the outcome of the stage 4 of the licensing process will be the SONS permission to permanent operation of this unit refurbished I&C systems important to safety.

The safety case documentation providing evidence that the applicable requirements of the design for safety have been met in the design and implementation of the refurbished I&C systems important to safety will have the format and contents as per the US NRC Regulatory Guide 1.70 and NUREG-0800/1997.

Present status of the licensing process

Stage 1A of the I&C system refurbishment project licensing process was completed at the end of 1999. Safety case of the stage 1B was submitted to the SONS in May 2000. Its assessment has been completed without any significant negative findings. The safety case of the stage 2 of the licensing process is going to be submitted for the regulatory assessment at the end of March 2001.

APPENDIX A.3.

FINLAND, COUNTRY REPORT
(provided by P. Haapanen, VTT)

Current Regulatory Practice and Industry Standards in Finland

1. HISTORICAL BACKGROUND

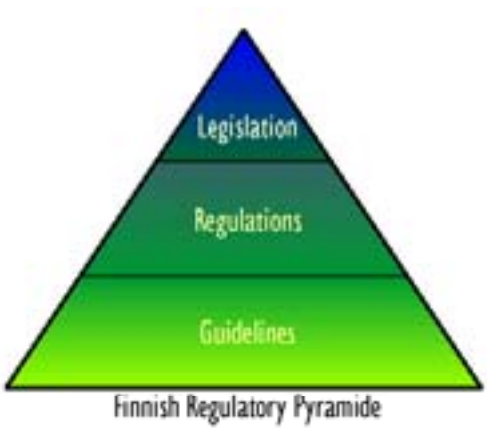
The safety and reliability problems associated with the software based automation systems were early recognised in Finland and some research projects were started already in the 1970's in co-operation with the OECD Halden reactor project, and have then continued inside the Finnish nuclear safety research programmes. A new automation system safety guide (YVL 5.5) accommodating the specialities of software based systems has also been under development at the safety authority (STUK) and will be launched still before the end of the year 2001.

Some safety related digital I&C systems have already been licensed and taken into operation during the last few years in Finnish nuclear power plants, mainly at the Olkiluoto BWR plant. These systems have officially been licensed under the old version of the YVL 5.5 guideline stemming from the year 1986, but the new requirements in the new version have also been taken into account as far as possible.

There are at the present two safety class 2 digital systems in operation at the Olkiluoto plant, namely the neutron flux monitoring system and the main circulation pump frequency converter control system. Further, there are two more safety class 3 digital systems, namely the turbine control and protection system and the control rod manoeuvring system.

Fortum, the owner of the Loviisa PWR plant, has recently started a comprehensive development project aiming at the possible replacement of the old hard-wired reactor protection system with a digital system during the next ten years.

2. REGULATORY FRAMEWORK



Finnish Regulatory Pyramide

A customary three-level hierarchical regulatory structure like in most nuclear energy exploiting countries has also been adopted in Finland as given in Fig. 1. A more detailed conception of the contents of the Finnish regulatory structure is given in Table 1.

On the top, the legislation level, they're the Nuclear Energy Act (990/1987) and the Nuclear Energy Degree (161/1988). The Nuclear Energy Act first stipulates the general prerequisites for using nuclear energy: "it shall be in line with the overall good of the society and it must be safe i.e. it shall not cause injury to people, or damage to the environment or property". It further defines a three level consent system being composed of the "Decision in Principle", "Construction License" and "Operation License" and defines the competent bodies for granting these. The Decision in Principle is taken by the Council of State and must then be accepted (or rejected) as such by the parliament. The Construction and Operation Licenses are also granted by the Council of State. According to the Act the Ministry of Trade and Industry is responsible of the highest Management and supervision of nuclear matters. The Radiation and Nuclear Safety Authority (STUK) is responsible for the supervision of the safe use of nuclear power.

The Nuclear Energy Degree supplements the Act by giving more detailed requirements e.g. for the contents and information needed in the applications for the Decision in Principle and the Construction and Operation licenses.

Table 1. The contents of the Finnish nuclear regulatory system

Legislation	Nuclear Energy Act (990/1987) Nuclear Energy Decree (161/1988)	
Regulations	Decisions of the Council of State (VNP) on the general regulations for the safety of nuclear power plants (395/1991) on the general regulations for physical protection of nuclear power plants (396/1991) on the general regulations for emergency response arrangements at nuclear power plants (397/1991) on the general regulations for the safety of a disposal facility for reactor waste (398/1991) on the safety of disposal of spent nuclear fuel (478/1999)	
Guidelines	The use of nuclear energy (YVL Guides) General (16) Systems (8) Pressure vessels (7) Buildings and structures (3) Other structures and components (8) Nuclear materials (12) Radiation protection (12) Radioactive waste management (4)	The use of radiation (ST Guides) General (5) Radiation Therapy (2) Diagnostic Radiology (6) Measurement of Radiation (1) Industry, Research, Education and Commerce (5) Unsealed Sources and Radioactive Wastes (2) Radiation doses and health surveillance (5) Non-Ionizing Radiation (4) Natural Radiation (3)

For the application for the Construction License the applicant shall submit the following documents to STUK:

- preliminary safety analysis report
- proposal for classification document
- description of quality assurance
- plans for physical protection and emergencies
- safeguards plan

For the application for the Operation License the applicant shall submit the following documents to STUK:

- final safety analysis report
- probabilistic safety analysis
- quality assurance program
- technical specifications
- programme for periodic inspections
- arrangements for physical protection and emergencies
- arrangements for safeguards
- administrative rules
- programme for radiation monitoring

The legislation level regulation does not contain any specific requirements for the automation systems but these are first met at the second level of the regulation hierarchy. This level, the regulation, consists of the five Decisions of the Council of State (VNP 395 – VNP 398/1991 and VNP 478/1999). For the licensing of the automation systems the most important regulation level document is the Decision of the Council of State No 395, which defines the general safety requirements. There are both general requirements for all safety systems and requirements specific to automation systems.

From the licensing of automation systems point of view especially the following requirements are of importance:

- Section 5, Quality assurance

Advanced quality assurance programmes shall be employed in all activities which affect safety and relate to the design, construction and operation of a nuclear power plant

- Section 13, Levels of protection

In design, construction and operation proven or otherwise carefully examined high quality technology shall be employed to prevent operational transients and accidents (preventive measures).

Effective technical and administrative measures shall be taken for the mitigation of the consequences of an accident. Counter-measures for bringing an accident under control and for preventing radiation hazards shall be planned in advance (mitigation of consequences).

- Section 19 Avoiding human errors

Special attention shall be paid to the avoidance, detection and repair of human errors. The possibility of human errors shall be taken into account both in the design of the nuclear power plant and in the planning of its operation so that the plant withstands well errors and deviations from planned operational actions

- Section 21, Safety classification

The systems, structures and components important to safety shall be designed, manufactured, installed and operated so that their quality level and the inspections and tests required to verify their quality level are adequate considering any item's safety significance

- Section 22, Monitoring and control of a nuclear power plant

A nuclear power plant's control rooms shall contain equipment which provide information about the plant's operational state and any deviations from normal operation as well as systems which monitor the state of the plant's safety systems during operation and their functioning during operational transients and accidents.

There shall be an emergency control post at a nuclear power plant which is independent of the control room and the necessary local control systems by the means of which the nuclear reactor can be shut down and cooled and residual heat from the nuclear reactor and spent fuel stored at the plant can be removed.

By virtue of the above acts and regulations, the Finnish safety authority, the Radiation and Nuclear Safety Authority (STUK) issues detailed regulations, the YVL guides, which form the third level of the regulation hierarchy. The publication of a YVL guide does not, as such, alter any previous decisions made by STUK. After having heard those concerned, STUK makes a separate decision on how a new or revised YVL guide applies to operating nuclear power plants, or to those under construction, and to licencees' operational activities. The guides apply as such to new nuclear facilities.

When considering how new safety requirements presented in YVL guides apply to operating nuclear power plants, or to those under construction, STUK takes into account section 27 of the Council of State Decision (395/1991), which prescribes that for further safety enhancement, action shall be taken which can be regarded as justified considering operating experience and the results of safety research as well as the advancement of science and technology.

If deviations are made from the requirements of the YVL guides, STUK shall be presented with some other acceptable procedure or solution by which the safety level set forth in the YVL guides is achieved.

The principal guide for the automation systems is the YVL 5.5: Automation Systems and Equipment for Nuclear Power Plants, but several other guides set requirements also on automation systems. Other guidelines directly referred to in the revised YVL 5.5 draft are given in Table 2.

Table 2. YVL- guides referred to in YVL 5.5

YVL 1.0	Safety criteria for design of nuclear power plants
YVL 1.1	Finnish Centre for Radiation and Nuclear Safety as the regulatory authority for the use of nuclear energy
YVL 1.4	Quality assurance of nuclear power plants
YVL 1.6	Nuclear power plant operator licensing
YVL 1.8	Repairs, modifications and preventive maintenance at nuclear facilities
YVL 1.9	Quality assurance during operation of nuclear power plants
YVL 2.0	General requirements for system design and supervision
YVL 2.1	Nuclear power plant systems, structures and components and their safety classification
YVL 2.2	Transient and accident analyses for justification of technical solutions at nuclear power plants
YVL 2.5	Pre-operational and startup testing of nuclear power plants
YVL 2.6	Provision against earthquakes affecting nuclear facilities
YVL 2.7	Ensuring a nuclear power plant's safety functions in provision for failures
YVL 2.8	Probabilistic safety analyses (PSA)
YVL 3.7	Pressure vessels of nuclear facilities. Commissioning inspection
YVL 4.3	Fire protection at nuclear facilities
YVL 5.2	Nuclear power plant electrical systems and equipment

The influence on automation of these guidelines is in most cases quite obvious. Therefore in the following only few of the most important are shortly described.

3. SAFETY CLASSIFICATION

The level of requirements in YVL 5.5 is attached to the safety classification of the subject in question. The principles of the safety classification of systems, structures and components are defined in YVL 2.1, which also includes in an appendix examples of safety classification for present day light water reactors. YVL 2.1 introduces four safety classes (1 to 4, 1 being the most demanding class) and a non-safety class YET. No automation functions/systems are located in safety class 1, so the class 2 is the highest for these systems. In an international comparison the Finnish safety class 2 is roughly corresponding the 1E class in the American or Cat A or the IEC 61226 classification and class 3 the non-1E or Cat B.

Essentially the YVL 5.5 guide concentrates on safety classes 2 and 3 for which the appendix of the YVL 2.1 gives the following classification examples

Class 2

A protective instrumentation and automation system for starting a reactor trip, reactor emergency cooling, isolation of reactor containment or other safety function necessary in a postulated accident.

Class 3

Instrumentation and automation systems and components required for the following functions and not classified to a higher safety class:

- reactor power limitation systems
- control of reactor main parameters (power, pressure, coolant volume)
- monitoring and control of safety functions during accidents
- monitoring and control of reactor power peaking
- monitoring and control of safe plant shutdown from the main and standby control rooms
- monitoring of reactor criticality during fuel loading
- monitoring of primary circuit leaks
- monitoring of hydrogen and oxygen concentrations inside the containment
- monitoring of primary circuit water chemistry
- on-site radiation monitoring during accidents
- monitoring of radioactive releases
- monitoring for radiation in rooms.

4. FAILURE CRITERIA

Failure criteria are defined in the guide YVL 2.7. For the automation system point of view the following criteria are the most important:

- fail safe
- single failure
- active and passive faults
- deterministic and probabilistic methods
- common cause faults
- diversity
- separation and segregation

5. RELIABILITY TARGETS

The guide YVL 2.8 contains the requirements for the Probabilistic safety analyses (PSA) and also defines some numerical design objectives for the most critical safety functions. The guide shall be proved to be fulfilled high a high confidence. The most important from the automation systems point of view is the requirement of the probability of failure on demand (pfd) to be less than 10^{-5} for the reactor trip function. This requirement is extremely hard to prove especially for a software based automation application and most probably requires the construction diverse redundant subsystems.

6. LICENSING PROCESS

The actual licensing process is defined in the guide YVL 5.5. The new version of the YVL 5.5 will be issued before the end of the year 2001. It will be applicable both for analogue and digital systems in contrast to the practice many other countries where special guidelines for digital systems alone have been written.

The new YVL 5.5 guide consist of a general introduction and five main chapters:

- design base for automation systems and components
- general design requirements
- design and implementation of automation systems
- ageing management
- supervision by the STUK

The design base mainly emphasises the requirements stemming from the Decision of the Council of the State (VNP 395/1991) and other YVL guides.

General design requirements contain conditions for:
- qualification for environmental conditions
- electromagnetic compatibility
- fire analysis
- data security

The requirements for the design and implementation concern e.g:
- quality control
- design process
  - requirement specifications
  - documentation
  - change control
- qualification plan
  - high quality design process
  - testing
  - analyses
  - operational experiences
  - type qualification
- special requirements for software based systems
  - base system qualification
  - programming tools design methods
  - pre-existing software (COTS) and equipment
  - avoiding and analysing common cause failures (CCF)
  - testing

A short chapter on ageing monitoring requires the licensee to establish a program for the assessment of the remaining life time and possible need for replacement of automation systems and equipment. This program shall include the collection and analysis of failure history. The choice of the systems covered by the program shall be justified.

The last chapter defines the supervision actions of STUK and the documentation the licensee has to provide to STUK for this purpose. The supervision actions are divided in phases so that the authority can make her decisions as early as possible. Important items in the supervision programme are the “Preliminary inspection materials” (ETA’s) that the licensee will provide to STUK before the end of the main phases of the design process. The main phases, documents and actions are:

Pre-inspection of the principal design based on the following documentation (for systems in safety classes 2 & 3):
- design principles and bases of the system
- functions, function principles and most important design parameters
- separation and segregation of systems and equipment and preliminary location in the plant
- preliminary safety classification
- environmental circumstances and loads of systems
- requirements and dependencies from other systems
- system interfaces

- preliminary qualification plan
- preliminary security plan
- quality control principles and the competencies of design partners
- preliminary safety assessment

Pre-inspection of system (for systems in safety classes 2 & 3 and some in 4)
- detailed design bases
- detailed function and architecture
- influences on and dependencies from other systems
- location, separation and protection (fire departments, physical protection) of subsystems important to safety
- probabilistic assessment of the implication of the system on the safety o the plant
- quality plan
- general data security plan
- qualification plan
- qualification results
- independent assessments
- safety assessment

Pre-inspection of equipment

STUK carries out equipment specific pre-inspection for the equipment belonging to safety class 2 and the central accident equipment belonging to safety class 3. The following documentation shall be provided to STUK for acceptance:
- equipment design bases
- suitability analysis

Further, the following documentation shall be provided to STUK for attention:
- plant and application specific requirement specification of the equipment
- function and construction descriptions and drawings of the equipment
- manufacturer information
- type acceptance report

STUK will also after own judgement supervise the manufacturing and factory tests, the installation and commissioning and the operation, maintenance and possible changes of the system belonging to the scope of pre-inspection.

7. STANDARDS AND GUIDELINES

The guide YVL 5.5 dos not explicitly define any set of standards and guidelines to be applied during the design, construction, commissioning, operation and maintenance phases of the lifecycle of the automation system. Instead, it states that selection and application of proper standards and guidelines is of the utmost importance for the high quality design (design process is here a broad concept covering the whole life cycle) process to reach the required high level of safety. For the applications belonging to the safety class 2 mainly nuclear standards, e.g. IEC 60880, IEC 60880 -2, IEC 60987 and IEC 60780 shall be applied when for the lower classes also general standards are applicable.

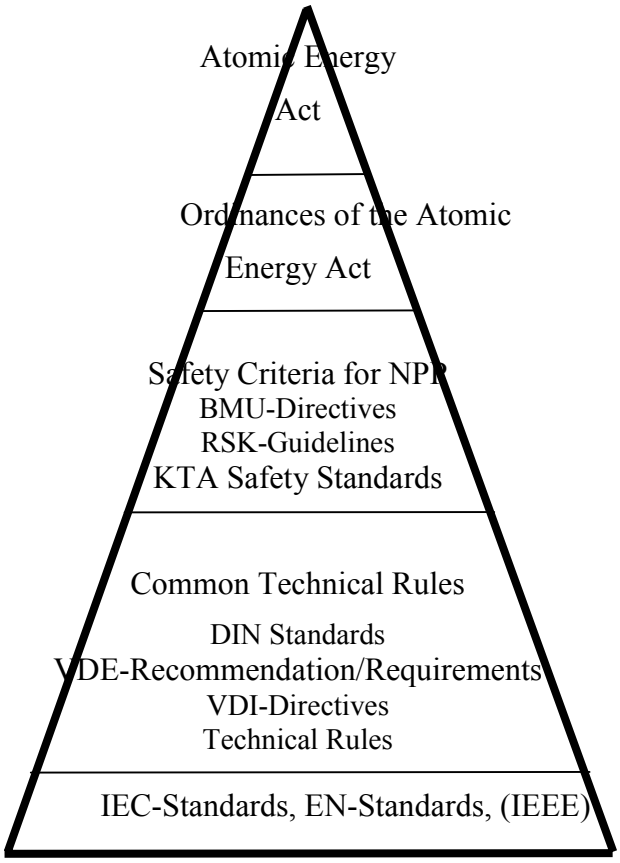
APPENDIX A.4.

GERMANY, COUNTRY REPORT
(provided by W. Bastl, H.-W. Bock/ Framatome-ANP and A. Lindner/ ISTech)

Current Regulatory Practice and Licensing Standards in Germany

1. BASIS FOR THE LICENSING APPROACH

The basis of the licensing approach is the "Act on the peaceful use of nuclear energy and the protection against its hazards" (Atomic Energy Act) with subordinated rules guidelines and standards.



Due to the federal structure of Germany, the state authorities are responsible for the licensing of nuclear power plants.

2. ASSESSMENT AND LICENSING OF COMPUTER BASED I&C

First applications of computer based I&C were introduced in the frame of minor up-grading projects, the associated assessment and licensing activities were performed on a case by case basis, with existing rules and guidelines (e.g. issued by KTA or the German Reactor Safety Commission – RSK) applied "according to the safety rationale" laid down in these documents. Since specific national standards and guidelines for digital I&C were not available, international standards, especially IEC 60880, have been used in addition. E.g. the

requirements of IEC 60880 have been applied in the type tests of the TELEPERM XS software performed from 1990 to 1998.

In order to address the safety issues of the new technology I&C systems more explicitly, Chapter 7 of the RSK Guidelines was completely revised in 1996 /1/. The main issues of this revision were

- the introduction of the protection goal (safety goal) approach as a means of demonstrating the fulfilment of the safety principles,
- the emphasis to be placed upon the requirement specification,
- the introduction of a classification system to allow for graded requirements according to the importance of the I&C functions and systems,
- The formulation of software requirements.

An overview of the contents of Chapter 7 is given in the Appendix.

2.1. Protection goals and auxiliary functions embracing the protection goals

The structure consists of four protection goals and five auxiliary functions embracing these goals. The protection goals and the principle tasks to be performed in order to meet these goals are (definition according to the Federal Office for Radiation Protection BfS /2/).

Control of Reactivity

The control of reactivity for all operational and accidental conditions is ensured

- if changes of the reactivity or of the local power density is limited to admissible values, through the inherent core properties together with the automatic actions of the control, limitation and reactor protection systems,
- reactor core shut down can be performed reliably,
- the fuel elements remain subcritical during handling,
- the fuel elements remain subcritical in the fuel storage tank.

Cooling of Fuel Elements

The cooling of fuel is ensured for all operational and accidental conditions, if the heat generated in the fuel can be removed. Therefore

- coolant and heat sinks have to be available,
- heat transport from the fuel to the heat sink has to be ensured,
- heat removal from the fuel storage tank has to be ensured.

Enclosure of Radioactive Substances

Enclosure of radioactive substances is ensured even for accidental conditions if

- the fuel remains sufficiently enclosed,
- leakages or cracks of the primary circuit pressure boundary are manageable,

- the integrity of the safety enclosure is ensured (safety enclosure = the containment and the associated building structures and the auxiliary systems for retaining and filtering of containment leakages).

Limitation of Radiation Exposure

The limitation of the radiation exposure is ensured if

- the activity inventory and activity flow in the plant remains limited and controlled,
- the release of radioactive substances is limited,
- the building structures and technical systems meet the requirements of radiation protection,
- radiation and activity is monitored in the plant and the environment,
- administrative rules of the radiation protection are recognised.

Auxiliary functions embracing the protection goals

Refer to the

- reliability,
- entire plant,
- administration,
- instrumentation and control,
- power supplies.

2.2 Protection goal approach

As a first step the process functions have to be identified which are necessary to meet the protectionsed upon the process functions the associated I&C functions important to safety can be defined. Depending on the safety importance of the functions and the associated reliability requirements, the I&C architecture (e.g. the degree of redundancy) is developed and appropriate equipment is selected to build up the I&C system.

In the course of licensing this design procedure has to be made transparent. It has to be demonstrated that the I&C important to safety is capable of meeting the protection goals by applying graded measures (defence in depth principle).

2.3 Requirement specification

As mentioned above a clear requirement specification is an important pre-requisite for defining the process and the related I&C functions. Moreover it provides the basis for grading the requirements for a classification system. Referring to the requirement specifications the RSK Guidelines state:

- All the requirements for the I&C important to safety shall be documented in the requirement specification; they shall be presented in a well structured way.

- The tasks of the I&C important to safety shall be identified by means of event sequence analyses, which include operational occurrences and accident conditions and considerations of plant internal emergency measures.
- The requirement specification shall structure the process tasks of the I&C important to safety in clearly separated sub-tasks of a limited/small set of functions. These sub-tasks have to be presented as I&C functions. The entire set of I&C functions shall be documented in a well structured way.
- For all the I&C functions the tasks, the classification in categories, the initiating criteria, control and actuation and signal acquisition shall be identified and documented.
- It shall be demonstrated, that the protection goals are met according to the requirement specification for all event sequences to be postulated.

2.4 Classification

When implementing the measures to meet the protection goals, the I&C important to safety includes functions of different importance to safety. According to the RSK Guidelines the I&C functions are classified in different categories for which graded requirements apply:

Category 1 relates to all I&C functions which are necessary to avoid non-tolerable consequences of accident conditions.

Category 2 relates to all I&C functions which are necessary to avoid the extension of operational occurrences/disturbances to accident conditions.

Category 3 comprises all the other I&C functions important to safety.

Corresponding to the safety importance of the I&C functions the devices implementing those functions are divided into classes with graded qualification requirements

Class E1 relates to all devices which carry out I&C functions of categories 1 and 2.

Class E2 relates to all devices which carry out I&C functions of category 3.

2.5 Software for I&C important to safety

According to the RSK Guidelines following basic requirements apply:

Software for I&C important to safety has to be developed according to a phase model, observing the following basic issues:

- The functions of application software and system software are to be implemented in autonomous software components. The software architecture shall assure a clear separation of application and system software.
- Software shall be designed such that no interference of lower ranked functions (with respect to safety) to higher ranked functions may occur.
- Programs must be robust and self-supervising.

- The correct execution of the programs is to be guaranteed independently of the transient behaviour of their input signals, e.g. by a deterministic, cyclic operation.

With reference to the categories the requirements are graded and structured following five aspects: principles, constructive QA, analytical QA, organisation and administration, use of standard software (e.g. operational system). Some examples to demonstrate grading are given below (for better visibility of the differences the concerned sentences are written in *Italics*).

Aspect "Principles"

Category 1

- The development and qualification of Software of category 1 *shall be designed such* that closed demonstration of correct operation of the software is guaranteed.
- Design and implementation have to be carried out on formal and computer-aided design and test methods which are also to be used extensively in the other development phases.
- Software of category 1 shall have a simple structure.
- The scope of functions of the SW of category1 shall be limited to the necessary extent.

In practise, for software implementing I&C functions of category 1, the requirements of IEC 60880 are applied in addition.

Category 2

- For the development and qualification of SW of category 2 computer-aided descriptions and test procedures shall be applied which support the demonstration of correct operation.

Category 3

- SW of category 3 is to be qualified according to recognized methods of SW engineering.

Aspect "Analytical QA"

Category 1

- The phase results have to be verified completely by formal analysis methods and additional tests, with regard to the requirements. In order to achieve this goal, at defined milestones examinations have top be performed.
- After installation on the processors, the behaviour of the hardware/software system shall be validated according to the requirements.

Category 2

- The phase results are subject to an examination and are to be documented. All safety relevant program parts have to be examined by a combination of test procedures by which a complete test coverage should be achieved.
- The behaviour of the hardware/software system shall be validated in its safety relevant functions according to the requirements.

3. RECENT DEVELOPMENTS CONCERNING STANDARDIZATION OF DESIGN REQUIREMENTS

In the framework of the project KTA 2000 a basic revision of the KTA rules has been agreed upon. The main idea is to generate a set of basic rules containing the principal safety requirements in the subject areas, as to achieve finally a roof of high level rules reducing system or equipment specific aspects as far as possible. Under this roof existing KTA rules will have the role to describe more specific requirements, and will therefore be streamlined and adapted to the basic rules and to the state of the art.

For all this adapting and up-dating efforts, existing standards (preferably DIN) will be utilized to the largest extent possible. In this context the decision of the KTA Subcommittee for Electrical and I&C Systems (KTA UA-EL) taken at its meeting on Nov. 14 and 15, 2001 is worthwhile to be mentioned, i.e. to upgrade the wording of the existing standards, but keep the alignment with analogue technology in accordance to the as-built status in the plants; the necessary extension to digital technology will be performed by citing relevant IEC standards. As direct citing of IEC standards is not possible for formal reasons, the relevant standards will be cited as DIN IEC norms after translation into German.

This means the IEC standards on digital I&C will ultimately cover important specific safety issues within the framework of the KTA basic rules. In addition one has to bear in mind the relationship between IEC SC45A standards and the IAEA codes and guidelines: According to the 1981 Agreement care is taken in tuning the activities of the projects in order to achieve consistency between the codes/guidelines and the standards, especially to fit the more detailed technical contents of the standards in the frame of the rather basic issues of the codes/guidelines.

Considering this situation the future role of IEC standards within KTA could be an important first step for international harmonization of the technical basis for licensing requirements.

4. LICENSING EXAMPLE

Framatome ANP is the owner of the TELEPERM XS system platform suitable for realising I&C systems important to safety. The system platform comprises the hardware, the software and a set of powerful engineering tools coping with all engineering phases relevant to software quality.

The principle to ensure a clear separation between platform related activities and those activities related to individual projects was one of the key issues for development and qualification of the platform.

Figure 4.1 gives an overview to the platform related qualification activities and the project related activities which have to be performed individually in each project.

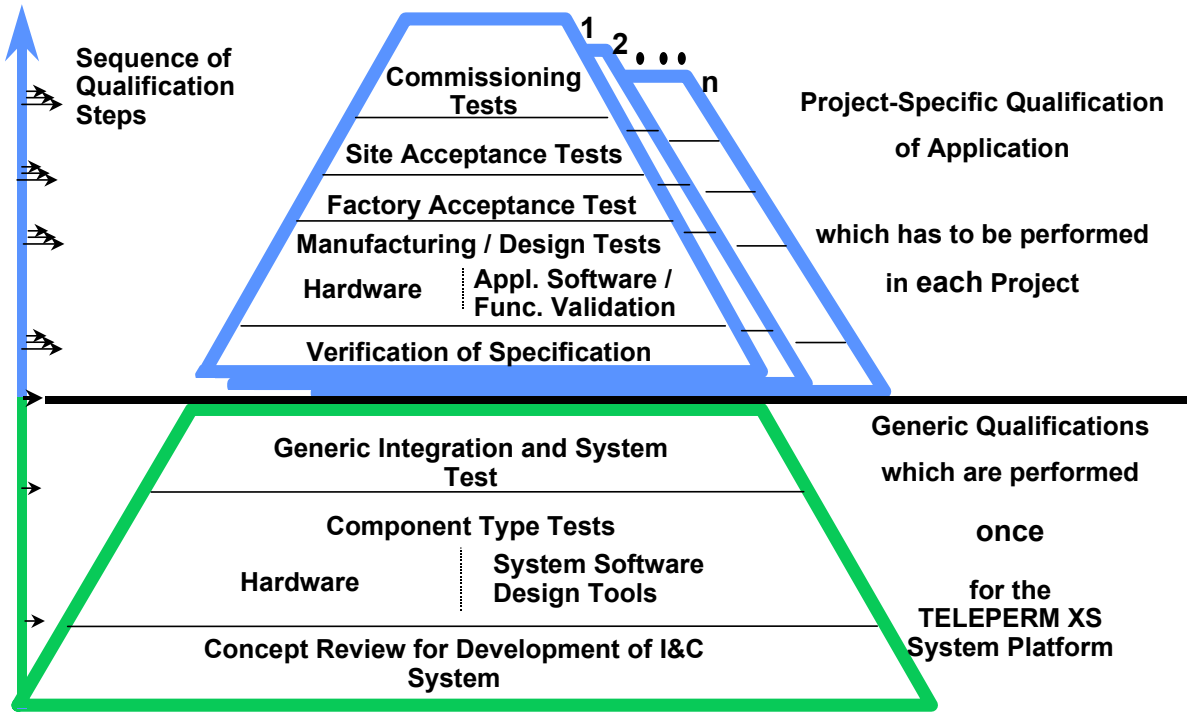


FIG. A4.1. Superposition of Generic and Project-Specific Qualifications.

By application of the qualified system platform TELEPERM XS each individual project has the advantage:

- not to be burdened by qualification costs related to platform features
- that the project specific engineered software meets highest quality requirements ensured by the use of the tool set and
- that the risk of project delays caused by unsolved problems from the licensing procedure is minimised.

The ***R***eactor ***P***rotection ***S***ystem (RPS) in the NPP Beznau was one of the recently finished upgrading projects (unit 1 in 10/2000 and unit 2 in 6/2001) using the system platform TELEPERM XS. Licensing was performed according to the requirement of the Swiss licensing organisation HSK by application of the German nuclear standards and requirements. For support the HSK placed a subcontract to the German TÜV Süd related to the technical assessment.

To cope with ***C***ommon ***C***ause ***F***ailure (CCF) functional diversity was applied. To achieve this the complete scope of protection functions was subdivided into two groups of functions which were implemented in two independent RPS-systems. The design requirements to ensure independence were discussed in a working group including experts of assessor and licensing bodies as well as customers and suppliers. The design requirements are published as VDI/VDE Guideline 2735 (Design criteria serving to ensure independence of I&C safety functions).

Figure 4.2 shows the fourfold redundant architecture of the installed systems including the related communication between their redundant subsystems and the communication to other systems. There are no communication paths installed between system A and system B. The independent RPS A and B process separate input-data by means of diverse application software which is based on the specification of diverse functions.

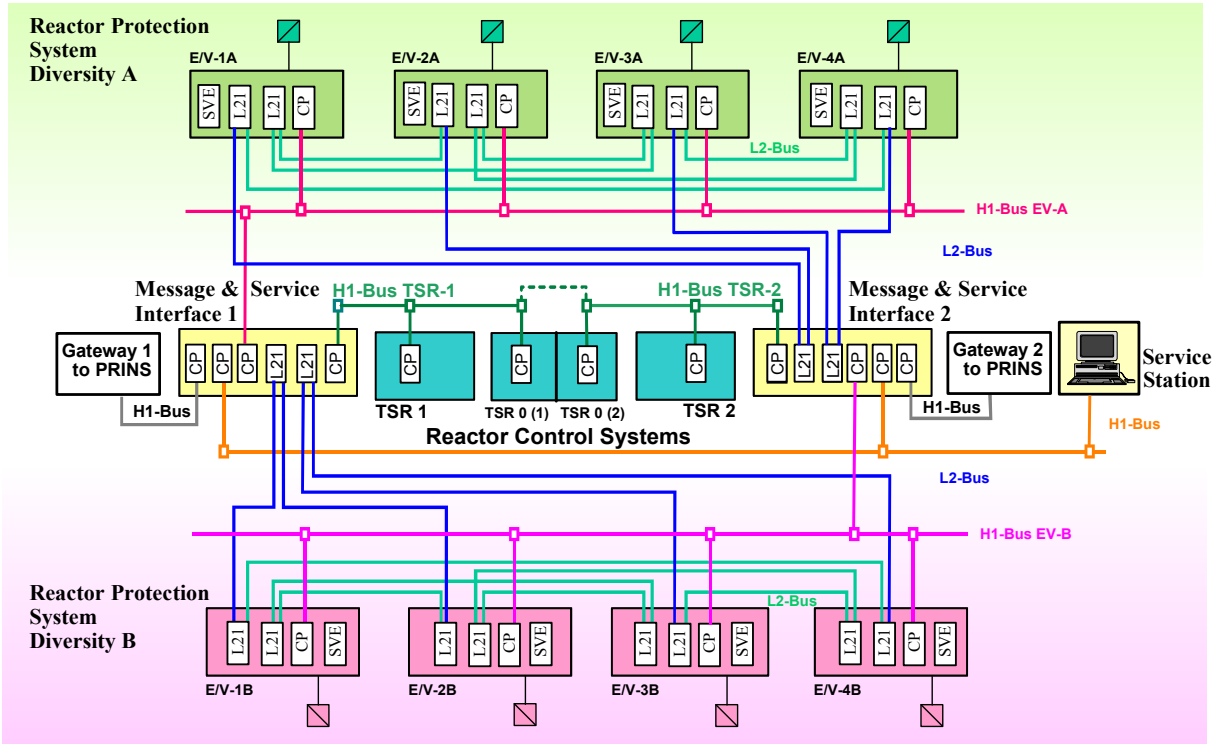


FIG. A4.2. RPS architecture in NPP Beznau.

REFERENCES

[1] RSK-Leitlinken für Druckwasserreaktoren, 3. Ausgabe vom 14. Oktober 1981, Neufassung des Kapitels 7 “Elektrische Einrichtungen des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung”.
Bekanntmachung von Empfehlungen der Reaktor-Sicherheitskommission vom 7.8.1996.

[2] Bundesamt für Strahlenschutz (BfS), Fachbereich Kerntechnische Sicherheit, Schutzzielorientierte Gliederung des Kerntechnischen Regelwerks.
Übersicht der übergeordneten Anforderungen (Dez. 1996) und Arbeitsgruppe Schutz-zielkonzept (BfS-KT-17/97).

Appendix: RSK Guidelines for PWR, Chapter 7, Electrical Equipment of the Safety System and the other Safety Relevant Systems

7. Electrical Systems of the Safety System and the other Safety Relevant Systems
   - 7.1 Scope
   - 7.2 General Requirements
     - 7.2.1 Design
     - 7.2.2 Inspections
     - 7.2.3 Documents to be Presented
   - 7.3 Safety Instrumentation and Control
     - 7.3.1 Scope
     - 7.3.2 General Requirements
     - 7.3.3 Requirement Specification
     - 7.3.4 Registration of Accidents and Disturbances
     - 7.3.5 Redundancy and Independence
     - 7.3.6 Qualification
       - 7.3.6.1 Qualification of the System
       - 7.3.6.2 Qualification of the Equipment
     - 7.3.7 Robustness
     - 7.3.8 Man-Machine Interface
     - 7.3.9 Inspection, Maintenance
   - 7.4 Electrical Components of the Safety System and of the Other Safety Relevant Systems
   - 7.5 Electrical Energy Supply of the Safety System and of the Other Safety Relevant Systems
   - 7.6 Safety Instrumentation and Control Software
     - 7.6.1 Requirements to be met by the Provision and the Examination of Software
       - 7.6.1.1. Software for the Safety Instrumentation and Control of Categories 1 to 3
       - 7.6.1.2. Safety Instrumentation and Control Software of Category 1
       - 7.6.1.3. Software for the Safety Instrumentation and Control of Category 2
       - 7.6.1.4. Software for the Safety Instrumentation and Control of Category 3
     - 7.6.2 Requirements for Operation and Security

APPENDIX A.5.

HUNGARY, COUNTRY REPORT
(provided by J. Eiler, Paks NPP)

Current Regulatory Practice and Industry Standards in Hungary

1. HISTORICAL BACKGROUND

The different safety functions and tasks provided in the original, Russian safety I&C system design were implemented in the following, autonomous subsystems:

- Reactor Technological Protection System (RTPS)
- Neutron Monitoring System (NMS)
- Emergency Core Cooling System (ECCS)
- Reactor Protection Central Cabinets (RPCC)
- Diesel Load Sequencer (DLS)
- Reactor Power Limitation System (RPLS)
- Steam Generator Protection System (SGPS)
- Loss of external electrical power supply automation

The requirements for the safety systems were in compliance with the Russian OPV 82 Standard. At the beginning of the '90s, there was an increasing expectation that an NPP should meet the continuously stricter safety and licensing requirements. Therefore, it was essential that the new protection system should meet the related national and international codes and standards, as well as the authority requirements.

The Paks NPP initiated the safety evaluation of the Reactor Shutdown System in 1992. The results of the study showed that the original safety systems were not in full compliance with certain national and international requirements. In spite of the fact that the studies focused on reviewing the functions of the Reactor Shutdown System, recommendations for the Emergency Core Cooling System upgrade were suggested, as well.

Besides this, a number of additional studies and safety analyses had been performed before the project started. In 1994, the AGNES Study (Advanced General and New Evaluation of Safety) was performed specifically for the Paks NPP. This study identified the deficiencies and weak points of the existing I&C systems.

In the period of 1999 to 2002, the Paks NPP replaced and schedules to replace the conventional, relay-based safety I&C systems of the nuclear Units with an integrated reactor protection system (RPS) based on the TELEPERM XS (TXS) digital equipment from Siemens. The new system integrates all the originally separated subsystems listed above and introduces several functional modifications.

2. BASIS FOR THE LICENSING

Figure 1. shows the structure of the Nuclear Regulations in Hungary. From practical licensing points of view, the third and fourth levels are the most significant ones. At the third level, the main Regulations are summarized in five books. Their breakdown is:

1. Regulatory Authority Procedures for Nuclear Power Plants
2. Quality Assurance Regulations for Nuclear Power Plants

3. General Design Requirements for Nuclear Power Plants
4. Safety Requirements for Nuclear Power Plant Operations
5. Regulations for Scientific and Research Reactors

To facilitate understanding and the interpretation of the regulations, the Hungarian Atomic Energy Authority (HAEA) has issued several Guidelines, coming down to the fourth level in the pyramid. These booklets give guidance, among others, for design changes and modifications. They contain detailed instructions on the licensing procedure to be followed and the documentation to be submitted to the authority. The number of Guidelines issued to date can be seen in the pyramid.

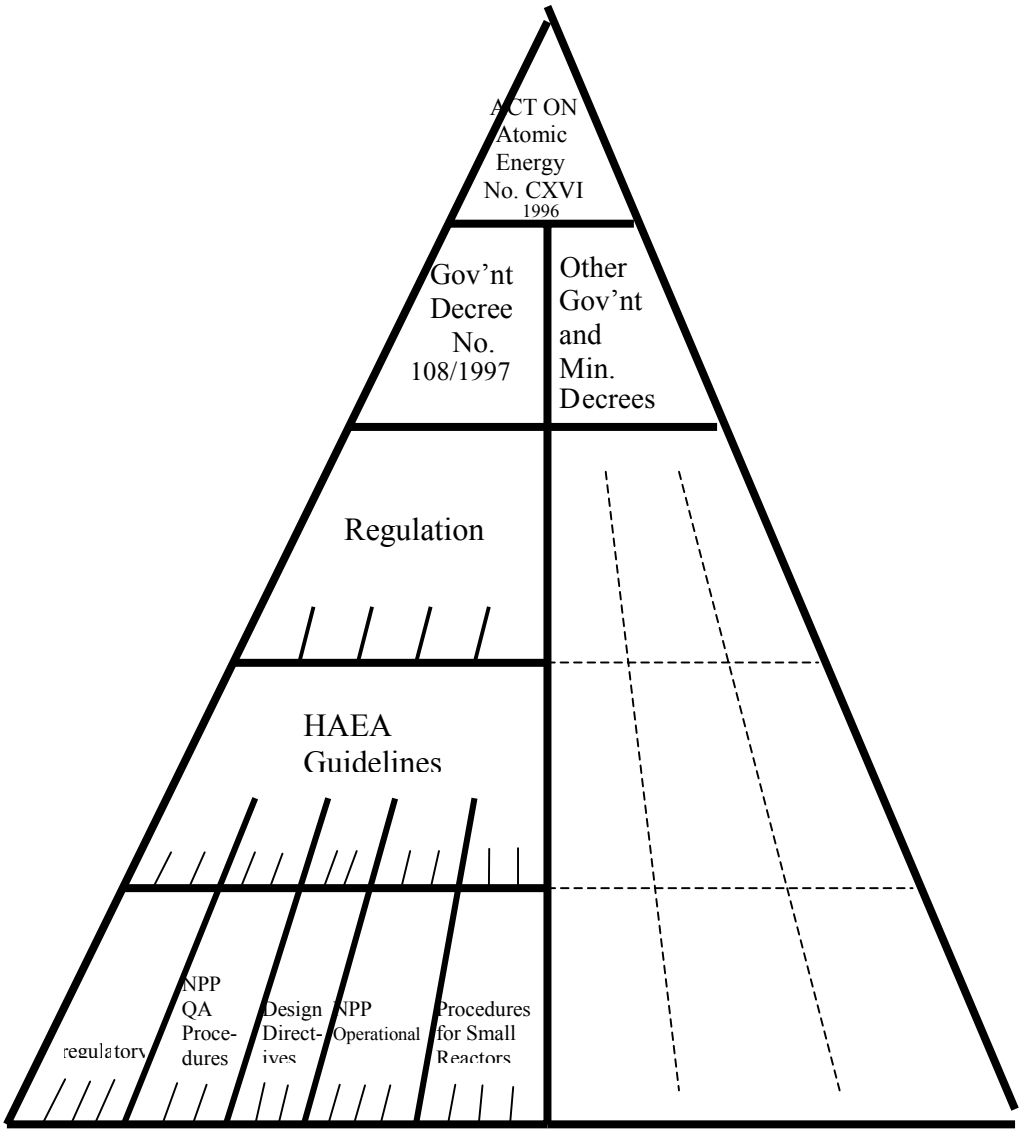


FIG. A5.1. Legal structure of the Hungarian Nuclear Regulations.

Regarding programmable, digital safety systems, there was no existing, specifically computer relevant standard in Hungary, except for the software specific part (9000-3) of the ISO-9000 series, which was translated and interpreted into the Hungarian language.

In the Hungarian licensing case, therefore, the Licensee (the Paks NPP) had an agreement with the Authority on the list of applicable standards, which later were introduced in the contract with the equipment designer and supplier.

The list of these standards is as follows:

IAEA50-C-D Code of Safety for Nuclear Power Plants: Design 1988.

IAEA50-SG-D3 Protection System and Related Features in NPPs 1980.

IAEA50-SG-D8 Safety Related Instrumentation and Control Systems for NPPs 1984.

IAEA50-SG-D11 General Design Safety Principles for NPPs 1986.

IEC68 Environmental Testing, Basic Environmental Testing Procedures

IEC231 General Principles of Nuclear Reactor Instrumentation 1967.

IEC231D Principles of Instrumentation for Pressurized Water Reactors 1969.

IEC671 Periodic Tests and Monitoring of the Protection Syst 1980.

IEC709 Separation within the Reactor Protection System 1981.

IEC780 Qualification of Electrical Items of Safety Systems for NPPs 1984.

IEC801-1.,2.,3.,4. Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment 1984., 1991., 1984., 1988.

IEC812 Analysis Techniques for System Reliability-Procedure for Failure Mode and Effects Analysis 1985.

IEC880 Software for Computers in the Safety System of Nuclear Power Plants 1986.

IEC980 Recommended Practices for Seismic Qualification of Electrical Equipment of Safety Systems for Nuclear Generating Plants 1989.

IEC987 Programmed Digital Computers Important to Safety for NPPs 1989.

IEC1131-1.,2. Programmable Controllers 1992.

Guide to Nuclear

Safety Code

Volume 3. "Safety requirements for the design of electrical and I&C system and equipment for nuclear power plants"

3. LICENSING PHASES OF THE RECONSTRUCTION PROJECT

Figure 2. shows the lifecycle model that was applied to this project. It is a slightly modified version of the proposed software lifecycle in IEC880. The modification consists of indicating a separate branch of activities on the left side for conventional I&C items.

The steps in the lifecycle can be grouped into the following phases:

- Project establishment
- Preparatory phase
- Design and manufacturing
- Installation and startup
- Operation

Based on the Regulations and Guidelines, the following licensing phases needed to be passed during the above listed project activities:

- Authority statement
- Principle system license
- Import permit
- Manufacturing permit
- Design change license
- Installation and startup permit
- Operation license

The large amount of documentation that needed to be submitted to the Authority was prescribed in the pertinent Guidelines for each type of license.

4. LICENSING IN THE SAFETY I&C SYSTEM REFURBISHMENT PROJECT

In 1993, the refurbishment project submitted the first version of the Task Specification. The Hungarian Atomic Energy Authority (HAEA) Nuclear Safety Directorate (NSD) formulated a **first time opinion** on the I&C refurbishment, and did not refuse the idea of installing a digital system for reactor protection functions. This regulatory position resulted in digital solutions for the Hungarian NPP units in the commercial bid. Four competing companies gave preliminary offers for computerized safety I&C systems.

A final requirement specification phase resulted in a very detailed specification, consisting of the customer's requirements and the system specifications recommended by the potential suppliers. Based on the results, an **authority statement** concerning the principal design change license was granted in September 1995. The statement was basically positive, with some general and specific comments facilitating the next licensing step.

Contract negotiations commenced with Siemens, who submitted the best bid. A regulatory body license, called principal system license was required as a pre-condition for signing the contract by the management of the NPP. Therefore, an application for that license was submitted to the Nuclear Authority. The **principal system license** was issued in the middle of 1996.

It can be noted that in this project the Hungarian party took the responsibility for the functional specification of protection algorithms, the technological and thermo-hydraulic aspects. At the same time, Siemens was responsible for providing that the integrated system and the loaded software representing the reactor protection functions meet the specification.

In the next step, the reliability analyses assumed that, for every EP1 actuation, functional diversity is introduced by using two separate, diverse initiation criteria, which are detected by physically separate, diverse sensors. These criteria were then processed in two different computers within each protection train. The Hungarian authority accepted the **list of the diverse initiation criteria** in 1996.

During the 1997 and 1998 refueling outages in Unit 1, preliminary installation activities were conducted, which were also carried on during operation (cable laying, etc.). The preliminary **installation permits** were acquired from the authority for this construction work.

All the hardware and software design was completed for the Unit 1 equipment in 1998. System integration concluded at the Siemens manufacturing site by the end of 1998. The factory acceptance testing took place in Erlangen (Germany) in the first quarter of 1999.

The regulatory approach relied very far on the institutional type testing results, which were certified by German State authority technical support organizations. Siemens conducted the first phase of factory acceptance testing, independently from the Purchaser.

Supplier's FAT program

- System Integration Tests
- Test procedure: I/O test
- Test of communication connections
- Test of the FAT computer connections
- Factory Acceptance Test Procedures
- Input signal selection algorithms
- Irrationality algorithm for input signals
- Cabinet monitoring system
- Bus and computer load
- Process input and output signals
- Information output signals
- Human Interface signals
- Power Supply Cabinets
- Relay actuation and check back functions
- Periodic tests with the Test Machine
- Functional tests according to the Synoptical Functional Diagrams

These all were open-loop tests. Representatives from the Hungarian licensing body witnessed the tests even in the absence of representatives from the Purchaser. When Siemens declared the equipment was suitable for the final FAT, the conduction of the tests was taken over by the Hungarian side.

Independent FAT program, performed by the Purchaser

- Validation of the functional requirements
- Functional tests according to the Synoptical Functional Diagrams
- Functional tests according to the wording of the functional requirements
- Validation of the detailed technical requirements
- System performance
- Accuracy
- Response time
- Human interface
- Information interface
- Fault tolerance behaviour
- Deterministic behaviour
- Independence
- Testability
- Self-testing
- Periodic tests
- Startup tests
- Security Constraints

Based on the FAT results, the Hungarian licensing authority issued the **import permit** for TELEPERM XS, and the equipment was delivered to the Paks site.

In this project the closed loop tests were done with the full scope plant simulator at the Paks site, with a so called representative configuration of the new safety I&C system. The role of the closed loop tests was mainly the validation of the technological functions.

Final installation took place after receiving the **design change license** from the authority and concluded in June, 1999. The total replacement of the input signal sensors and transmitters took also place at this same time. Modifications to the control circuits of actuation devices were also necessary. Startup and commissioning took about two months and concluded in August, 1999, successfully. After a three-month trial operation, the authority issued the permanent **operation license**.

According to the experiences to date, the theoretical error calculations on the different modules resulted in a worse reliability than real life operation shows. TELEPERM XS behaves better in operation than it was calculated with a conservative approach.

APPENDIX A.6.

REPUBLIC OF KOREA, COUNTRY REPORT
(provided by B.R. Kim, KINS)

Current Regulatory Practice and Industry Standards in Korea

1. BASIS FOR THE LICENSING APPROACH

A regulatory authority, "Ministry of Science and Technology" in Korea and the Korea Institute of Nuclear Safety have approved and applied the nation's criteria of supplying reactor facilities in accordance with Minister's Notice No. 83-5, "Criteria for Location, Structure, and Components of Reactor Facilities". The review approaches in the process of licensing digital I&C systems have been emphasized on how to comply with relevant provisions of the Korean Atomic Acts and the fundamental acceptance criteria of U.S. 10CFR 50, Appendices A and B. In particular, with respect to digital I&C systems important to safety, the KINS requires the current requirements and guides applied to analog I&C systems, and also the specific positions regarding digital technologies. And the new Standard Review Plan (NUREG-0800) is a technical reference. The major licensing issues regarding digital I&C systems are safety classifications, software quality control including verification and validation, defense-in-depth and diversity analysis, qualification of electromagnetic environment, independence of data communication, etc.

2. EXAMPLE OF A TYPICAL LICENSING PRACTICE

Digital technologies have been gradually adopted to the safety-related Interposing Logic Systems at the starting point with YGN units 3 and 4. For Kori unit 1, due to component obsolescence, high maintenance costs and aging concerns, the upgrades of NSSS protection signal processing and bistable circuitry were implemented using commercial grade digital process instrumentation. The Plant Control Systems of Ulchin units 3 and 4 including interposing logics utilized microprocessors-based designs. All the protection systems, including reactor trip systems and ESFAS, of Ulchin units 5 and 6 under construction are being designed using digital technologies for the first time in Korea. The licensee submitted Safety Analysis Reports, software products and documents including software hazards analysis in accordance with software life cycle, and various qualification reports including EMI/RFI tests.

3. KEY REQUIREMENTS USED IN THE EXAMPLE

Defense-in-depth and diversity analysis

Defense-in-depth and diversity analysis for the reactor protection systems using digital technology shall meet the U.S. NRC positions regarding D-I-D and diversity described in the Staff Requirements Memorandum on SECY-93-087.

Software category and requirements

The software important to safety is classified into 3 categories; safety-critical, safety-related, and non-safety-related software. The safety-critical software shall meet the most

stringent standards and criteria with respect to hardware and software. If it is likely to occur common mode failures in the safety-critical software, a diverse backup system independent of the failures shall be provided. The safety-related software may be subject to less stringent practices and graded requirements than safety-critical one. The requirements of non-safety-related software may be tailored to account for the lower safety importance. The major differences among 3 software categories lie on the extent and severity in verification and validation activities, software safety hazard analysis, configuration management activities, and quality assurance activities to be performed during software development life cycle.

Qualification of pre-existing software

All pre-existing software, including operating systems, residing on digital I&C system computers at run time shall be qualified according to the importance to safety classification. However, the pre-existing software may be not qualified to meet the requirements in accordance with software category. In such a case, the risk analysis regarding the pre-existing software must be performed to demonstrate that the software does not have an impact on system safety. And some factors compensating for the missing elements of the software development life cycle shall be taken into account. Guidance on these activities is referred to EPRI TR-106439 or IEEE Std. 7-4.3.2-93.

Software safety hazard analysis

A planned and documented safety hazard analysis regarding the safety-critical software shall be performed during each phase of the software development life cycle. The analysis must ensure that the system safety requirements have been correctly addressed, no new hazards have been introduced, and software elements that can affect on safety are identified, etc.

Qualification of electromagnetic environments

Basically, the site surveys should be conducted. Electromagnetic measurements were performed at the power circuits to establish the conducted noise level that can be utilized as to the electromagnetic environmental test limit. The qualification of electromagnetic environments shall comply with EPRI topical report TR-102323-R1, as augmented by Mil-Std-461D and Mil-Std-462D.

Data communications independence

The independence between redundant channels of the safety system and between safety systems and non-safety systems shall be maintained as required. The preferred approach to communication independence ensures that redundant safety-grade equipment communicates via one-way communications paths and safety-grade systems do not receive information from non-safety-grade systems except when under test. In particular, the data flow to other channels is unidirectional broadcast to ensure communications independence. The in-channel communication is bi-directional only when under test to notify the logic testing to the other three channels. The communications to other channels can be implemented with fiber optic cables to provide electrical isolation between channels.

4. CATEGORIZATION TABLE FOR THE EXAMPLE

Plant	System/ Function	Backup System	Remarks
YGN 3&4	DILS/ Safety related functions at the component level	Hardwired Manual system	Intel 8085 CPU(8 bit) : Assembler language
Ulchin 3 &4	DPCS/ Safety related functions at the component level	Hardwired Manual system	32 bit Motolora CPU: Assembler language
Kori 1	Process protection system	No backup system	32 bit CPU : PL/M 86 Assembler language
Ulchin 5&6	Reactor Protection System/ ESFAS at the system level	DPS Hardwired manual system	32 bit Motolora CPU: AMPL language
	DPCS safety related functions at the component level	Hardwired manual system	Intel 386 Ex 32 bit CPU: PL/M 86 Assembler language

APPENDIX A.7.

UNITED STATES OF AMERICA, COUNTRY REPORT
(provided by H.M. Hashemian / AMS)

Digital I&C Implementation in US Nuclear Power Plants

I. INTRODUCTION

Digital I&C implementation in nuclear power plants continues to be a source of discussion and debate in the I&C community in the USA. Although there is great interest in digital I&C, the progress toward implementation of digital I&C for critical applications in nuclear power plants have been slow in the United States. This is due to a number of factors, including licensing difficulties. However, the learning curve of the nuclear industry in the area of digital I&C has been steep over the last ten years as evidenced by the number of meetings, technical papers, and conferences that include digital I&C in their agenda. For example, the Electric Power Research Institute (EPRI) has held numerous technical meetings in this area. In addition, digital I&C has been the topic in other forums such as the following:

1. 44th Annual Conference of the Power Industries Division of the Instrumentation, Systems, and Automation (ISA) Society, Orlando, Florida, July 2001.
2. Conference on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies for Nuclear Power Plants (NPIC & HMIT Conference), Washington, D.C., November 2000.
3. NPIC & HMIT Conference, Penn State University, Pennsylvania, May 1996.
4. National Research Council Report "Digital I&C Systems in Nuclear Power Plants" Safety and Reliability Issues, 1997.

In addition, the interest in digital I&C equipment for nuclear power plants is evident in an increasing number of suppliers who have developed, validated, and applied for NRC approval to provide digital I&C equipment to nuclear power plants. Although the number of suppliers of digital I&C equipment for important applications in nuclear power plants is still small; over the last five years, the choices of digital I&C equipment and suppliers have increased.

2. DIGITAL I&C ISSUES

In USA, the primary issues with digital I&C for nuclear power plants include:

1. Concerns with software common cause failure. In digital equipment, the same software module may be used in multiple systems including redundant instrument channels. As such, there is concern that a problem in a common software module can affect a number of equipment, compromise redundancy, and challenge the safety of the plant.
2. Electromagnetic and Radio Frequency Interference (EMI/RFI) effects on digital processors and integrated circuits.
3. Use of commercial products (e.g. software modules development for non-nuclear applications).
4. Subtle failures of digital equipment, isolation issues, and obsolescence.

Because of these and other concerns, digital I&C equipment, including test equipment, are subject to rigorous testing and verification and validation (V&V) programs. These testing programs are often carried out under a formal Quality Assurance (QA) program such as one that complies with 10CFR50, Appendix B. Furthermore, there are numerous guidelines and procedures for testing of digital equipment, software V&V, and software failure detection. In particular, EPRI has produced a number of useful guidelines in this area in addition to utilities, vendors, and the NRC.

3. REGULATORY DOCUMENTS ON DIGITAL I&C

The key U.S. regulatory documents on digital I&C include:

1. The Standard Review Plant (NUREG-0800). Chapter 7 of NUREG-0800 is concerned with nuclear plant I&C. This chapter includes a number of Appendices. Appendix 14 is on digital I&C and is commonly referred to as BTP-14 where BTP stands for Branch Technical Position (BTP) referring to the NRC's I&C branch in the office of the Nuclear Regulatory Regulation (NRR).

2. (10CFR 50.59). This document defines the U.S. law on the subject and is found under title 10 of the U.S. Codes of Federal Regulations (CFR).

3. NRC Regulatory Guide 1.152 endorsing IEEE 7-4.3.2.

4. NRC RESEARCH EFFORTS

The NRC has sponsored a number of research projects in the 1990s on nuclear plant I&C issues, including digital I&C issues. For example, a number of research efforts were funded by the NRC on aging of nuclear plant temperature and pressure sensors. These efforts included aging management techniques such as RTD and pressure transmitter response time testing, cross calibration of RTDs and thermocouples, cable condition monitoring, etc. Also, the NRC has sponsored a number of research projects at the Sandia National Laboratory and elsewhere on aging of cables, especially I&C cables. The emphasis on I&C cables has been due to concerns over the qualification of aged I&C cables in post accident conditions. The NRC research on digital I&C has centered around a number of issues, especially, environmental effects on digital I&C such as EMI/RFI, smoke, etc.

According to an NRC paper that was presented at the NPIC&HMIT Conference in November 2000, the NRC will continue its digital I&C research to help in improving the efficiency and effectiveness of its regulatory program. The NRC research will address a number of areas, including the following:

a. Digital I&C failure modes

b. Risk based regulatory program for I&C licensing

c. Development of more efficient methods and tools for regulatory review of digital I&C systems

Over the last few years, the NRC research on digital I&C has included a variety of important topics such as:

a. System aspects of digital technology (e.g. environmental stressors)

b. Software QA (e.g. software testing criteria)

c. Risk assessment of digital I&C (e.g. digital reliability assessment)

d. Emerging I&C technology and applications (e.g. predictive maintenance and on-line monitoring systems, advanced sensors, etc)

5. DIGITAL TEST EQUIPMENT

Although there is not an abundance of digital I&C equipment in nuclear power plants, digital technology has found many applications in nuclear power plants when it comes to test equipment to verify the performance of the plant and its components. For example, automated and computer-aided testing have found it's way well into testing activities in nuclear power plants. For example, rod drop time measurements in PWR plants were performed in the past on one rod at a time using a strip chart recorder. Today, the tests are performed on many rods at a time using digital test equipment and computers that perform the tests automatically, provide a report of the results instantly, and help in the documentation of the work and trending of the data. As a result, the rod drop test time is reduced from typically about eight hours to less than one hour. This provides significant cost savings to the plant by reducing the critical path time toward startup.

In July 2000, the NRC approved (with some stipulation) the on-line monitoring approach for extending the calibration intervals of pressure transmitters in nuclear power plants. This is another example of implementation of digital test equipment in an important application in a nuclear power plant. The details of on-line calibration monitoring are provided in NUREG/CR-6343 titled, "On-Line Testing of Calibration of Process Instrumentation Channels in Nuclear Power Plants." Additional examples of digital test equipment for nuclear power plants are found in NUREG/CR-5501 titled "Advanced Instrumentation and Maintenance Technologies for Nuclear Power Plants."

APPENDIX A.8.

SWEDEN, COUNTRY REPORT

**(provided by O. Andersson/ Forsmarks Kraftgrupp AB,
Bo Liwång /SKI)**

Regulatory Practice and Industry Standards in Sweden

1. HISTORICAL BACKGROUND

In Sweden, nuclear technology started in 1947, when AB Atomenergi was constituted to carry out a development programme decided by the Parliament. Consequently, the first reactor went critical in 1954. This was followed by the first prototype power plant Ågesta, which was operated from 1964 until 1974, when it was decommissioned. The first commercial nuclear power plant was started in 1972 and was followed by additional 11 units in the period up to 1985. The twelve commercial reactors constructed in Sweden comprise nine BWR: s (ABB design) and three PWR: s (Westinghouse design).

The development of nuclear power has since the TMI-accident, largely, been influenced by political decisions. The most important decisions were the final closure of Barsebäck unit 1 and extension of the time limit for decommissioning the remaining units beyond the year 2010, which was previously the target date for nuclear phase-out in Sweden. Another factor strongly influencing the recent development of the Swedish nuclear power industry is the deregulation of the electricity market and the further increase of competition, resulting in a strong pressure to reduce costs.

The safety requirements for Swedish nuclear power units was from the beginning based on American rules and regulations that existed at the time for the design of a specific unit, i.e. 10CFR50 (primarily Appendix A, General Design Criterion, GDC), Regulatory guides division 1 and guidelines issued by e.g. IEEE, ASME and ANS.

The application of each guideline and standard is described in the Final Safety Analysis Report (FSAR) which in turn was approved by the licensing authority before a license to operate was granted by the government. The implication of this situation is that the safety requirements are different for each unit, depending on which generation the specific unit belongs to. By the coming into force of a new general safety regulation in 1999, the licensing system has become more uniform. The new regulation does not only focus on traditionally safety aspects of a design. It also requires that the design solutions shall be adapted to the personnel's ability to, in a safe manner, manage the facility as well as the abnormal events, incidents and accidents that can occur. This requirement, together with utility experience, has put focus on the design requirements for the Human – Machine – Interface.

Since none of the Swedish units were originally equipped with software based systems for safety applications, none of the FSAR did contain licensing requirements for such systems from the beginning. As modernisation and backfitting projects come into focus supplementary, requirements have been added to the FSAR at all units in Sweden. Examples of such added requirements are provided below.

The perspective of operating the present plants for a longer time has initiated development programmes for defining adequate safety levels to be required for extended operation. Projects with this purpose have been pursued by both the regulatory body (Swedish Nuclear Power Inspectorate, SKI) and by the industry. These projects will also deal with safety requirements for software based functions.

2. REGULATORY FRAMEWORK

National law

The nuclear legislation in Sweden comprises the Act on Nuclear Activities (1984:3), the Radiation Protection Act (1988:220) and the respective Ordinances on Nuclear Activities and Radiation Protection. The Act on Nuclear Activities was amended again 1 January 1999 with provisions connecting to the Environmental Code which entered into force also 1 January 1999. In the licensing of nuclear activities, the general rules as well as the environmental norms of the Code apply. In addition, a license application shall always include an environmental impact assessment. SKI can also require such an assessment in other applications, according to the Act.

The licensing of nuclear facilities has become more complex since the Environmental Code came into force. For plants already licensed the new rules apply for instance when a new owner applies for transfer of the old license.

The Act on Nuclear Activities includes the basic legal requirements on licensing, and legal sanctions to be imposed on anyone who conducts nuclear activities without a license. For major installations and activities, the government on the recommendation of the regulatory bodies grants the license. The regulatory bodies license minor modifications and backfitting projects. For such minor modifications does neither the Act on Nuclear Activities nor the Environmental Code have any direct impact.

For all existing Swedish nuclear power plants, the licenses are valid without time limit. Licensing conditions can however be limited in time and in such cases, the time limits function as control stations. If the licensee complies with all legal binding safety requirements, a prolongation of the license cannot be denied in principle. A license can be permanently revoked if license conditions are not complied with, or for other serious reasons. Revoking a license for other reasons than safety, as in the Barsebäck 1 case, a special law is required.

National safety regulations

The general safety regulations of SKI "Regulations concerning safety in certain nuclear facilities" (SKIFS 1998:1) entered into force on 1 July 1999. These regulations are further described below. Other regulations formally issued by SKI are:

- Regulations concerning the competence of operations personnel at reactor facilities (SKIFS 2000:1).
- Regulations concerning mechanical components in certain nuclear installations (SKIFS 2000:2)

SKI plan to issue the following regulations:

- Safety in final repository of nuclear waste
- Physical protection of nuclear facilities
- National non-proliferation control
- Safety in transport of nuclear material and nuclear waste

- Safety of nuclear fuel and core management in reactor facilities
- General recommendations on the application of SKIFS 1998:1 regarding design and construction of reactor facilities (backfitting guidelines)

3. REGULATIONS CONCERNING SAFETY IN CERTAIN NUCLEAR FACILITIES, SKIFS 1998:1

Principles

The principles and logic behind the general safety regulation reflect the current regulatory philosophy in Sweden. In the regulations, three different control principles are used:

- Approval from SKI of the basic licensing documentation is required. This documentation is specified in the regulations: the (Final) Safety Analysis Report (SAR), the technical specifications, the emergency preparedness plan and the physical protection plan. A decommissioning plan must also be approved by SKI. In these cases and in other cases where an application is submitted, according to the Act on Nuclear Activities, SKI performs an in-depth technical review.
- Notification to SKI is required regarding all principal modifications in the mentioned documentation and in the plant itself. These modifications shall be subject to a twofold safety review by the licensee before SKI is notified. The safety review minutes shall be included in the notification. As soon as SKI is formally notified, the licensee is allowed to implement the modification. SKI is free to decide whether to review the notification or not. In all cases, further or other conditions can be imposed on the modification.
- SKI does not routinely interfere in any other safety issues. The licensee controls these through self-inspection. This self-inspection shall be supported by a strong quality management system, including strong systems for primary and independent safety reviews, subject to regular internal audits. SKI supervises the quality of the self-inspection. Incidents must of course be reported.

In addition to the three basic control principles there is a fourth principle concerning third part control in the SKI regulations on mechanical components (SKIFS 2000:2). This has, among other things, to do with the requirement to use non-destructive test methods qualified by an accredited inspection body and that such body certifies the achieved results.

Previously Sweden applied the same procedure as most other countries such that all plant modifications and modifications of the SAR and the Technical Specifications document must be submitted for approval (licensing) by the regulatory body. A reason for changing the scheme was a clearly felt need to concentrate the regulatory review resources on the most important issues for safety. The notification procedure allows this, but SKI still maintains control over the modification activities of the licensee. Another reason was to make the responsibility for safety more clear.

There are at least two fundamental prerequisites needed in order for a system with notification and self-inspection to be acceptable to the regulator. The first is a very clear nuclear law concerning the responsibility for safety. The Swedish Act on Nuclear Activities is very clear on this point. The licensee has total and undivided responsibility and must take any initiative which might be needed to maintain safety. The other prerequisite is that the regulatory body has confidence in the capability of licensee to perform self-inspections. It must be verified that adequate resources, competence and work practices are in place.

The new system has been in use more than two years and the over all experiences are:

- It has been necessary to adapt the regulators internal practices to the new rules. A standing group of experts from different SKI departments has been established in order to make a first assessment of all notifications. The group makes a proposal to the reactor safety management meeting regarding each notification:
  - No further action, or
  - the notification should be further reviewed in specific aspects.

For this first assessment, a set of criteria has been developed based on the safety significance of the notification, other relevant circumstances, and the degree of confidence SKI has in the self-inspection of the licensee. For instance, if a notification has to do with new or complex technology, like software based I&C systems, there is a high probability that this notification will be reviewed further. The head of the responsible office makes the final decision whether to review or not.

- After some initial problems, the notification routines are now running smoothly. Occasionally SKI has returned notifications to the licensee with a request for more information in order to decide to review or not. In a number of cases, SKI has not been satisfied with the quality of the safety reviews submitted. However, the general experience is that the quality has improved over time and is now satisfactory.
- In the opinion of SKI, the objective with the new system has been achieved, even if further fine-tuning is needed. More notifications have been reviewed than originally planned but this is normal when launching a new system.
- In addition, the licensees have declared a general satisfaction with the system. The responsibilities are clear and it is felt that the response time of the regulatory body is much shorter than before.

Regulations on plant modifications and safety review

The requirements within "Regulations concerning safety in certain nuclear facilities, SKIFS 1998:1" focus, as regards I&C, on the personnel's ability to manage the facility during different operating states. The technical requirements are more general and does not address software based I&C explicitly.

Within the "Regulations concerning safety in certain nuclear facilities, SKIFS 1998:1", the following paragraphs regulates plant modifications and the safety review that the licensee shall perform:

Chapter 3, Design and construction

In order to met the requirements of Chapter 2 §1 (basic safety requirements), the design of the facility, with adaptation to the specific conditions of each facility shall:

- be able to withstand component and system failures,
- have reliability and operational stability,
- be able to withstand such events and conditions which can affect the safety function of the barriers or defence-in-depth, as well as,
- have maintainability, controllability and testability of inherent parts as long as these parts are used for their intended purposes.

Comment: The design basis requirements which are specific in the regulations are of a fundamental nature and must, to the appropriate extent, be taken into account during all design work, before a facility is taken into operation as well as in connection with later plant modifications.

Ability to withstand such events or conditions that can effect the function of the barriers or the defence-in-depth system, refers to events or conditions which, in safety assessments, have been found to affect the safety function in a significant way. Examples of such events or conditions may be pipe break, transients, fire, flooding, earthquakes, clogging of cooling water intakes, sabotage and disturbances in or loss of the offsite power grid.

Chapter 3, Design and construction

Design principles and design solutions shall be tested under conditions corresponding to those which can occur during the intended application in a facility. If this is not possible or reasonable, they must have been subjected to the necessary testing or evaluation with reference to safety.

Comment: The provisions in this section include environmental qualification in the form of documented tests to ensure that components in equipment that is of importance for safety function as postulated in the safety report. In order to meet this requirement, it is important that such qualification should be performed taking into account normal operating conditions as well as conditions which arise in connection with abnormal events, incidents and design basis accidents.

Chapter 3, Design and construction

The design solutions shall be adapted to the personnel's ability to, in a safe manner, manage the facility as well as the abnormal events, incidents and accidents that can occur.

Comment: The design solutions should be adapted to the functions and tasks which are to be carried out as well as to the possibilities and limitations of human beings. Experience from the facility in question and from the personnel should be taken advantage of at an early stage and experts on man-technology-organisation interaction should be hired to take part in the design, analysis and evaluation of different solutions.

Special attention should be paid to ensuring that the safety systems are designed so that there is enough time for consideration and time for executing the operator actions that affect the safety functions. Particular attention should be paid to the information and alarm systems of the control rooms. The personnel should have access to the information that is necessary at different operating states without becoming overloaded by information during abnormal events, incidents, accidents or refuelling outages. Furthermore, the man-machine interface should be designed in accordance with accepted ergonomic practice, so that the interface is compatible with human conditions as well as satisfies the need for interaction and communication during work. The solutions that are developed should be evaluated in the context where they will be used.

Chapter 3, Design and construction

Building components, devices, components and systems shall be designed, manufactured, installed, controlled and tested in accordance with requirements which are adapted to their importance for safety.

Comment: In order to ensure that building components, devices, components and systems are as well adapted as possible to their importance for safety, a classification system should be applied for controlling requirements with respect to design and quality control.

In this context, control refers to the quality control that is needed in order to ensure that no faults or deviations remain in individual parts as well as to such performance and operational testing that is necessary in order to ensure that the devices and systems can fulfil all of the safety functions concerned in a reliable manner during normal and abnormal events and incidents as well as during possible accident situations.

Chapter 4, Assessment and Reporting of the Safety of Facilities

A safety review shall determine or control that the applicable safety-related aspects of a specific issue have been taken into account and that appropriate safety-related requirements with respect to the design, function, organisation and activities of a facility are met. The review shall be carried out systematically and shall be documented.

A safety review shall be performed within the parts of a facility's organisation which are responsible for the specific issues as well as within a safety review function appointed for this purpose which shall have an independent position relative to the parts of the organisation which are responsible for the specific issues.

Comment: In order to fulfil the requirement on a comprehensive review, the safety review should comprise a review of technical factors as well as a review of the man-technology-organisation interaction (human factors). Thus, personnel with technical competence within the areas in question as well as personnel with competence in behavioural sciences should participate in this work.

The primary safety review should always be carried out within the part of the organisation that is responsible for a particular safety case. This review of a specific issue should be as comprehensive as possible and should not take into account the fact that there will also be an independent safety review. The independent review should, in the light of how an issue has been handled within the responsible parts of the organisation, determine whether the applicable safety aspects have been taken into account and whether applicable safety requirements are fulfilled. Thus, an evaluation should be made of whether the analyses upon which the reported conclusions are based have been carried out with the adequate depth and adequate technical quality.

Thus, the intention of an independent safety review is largely to evaluate or control that an issue has been handled in a satisfactory manner from the standpoint of safety and is not intended to be a repetition of the primary safety review of the specific issue carried out by the responsible part of the organisation. This also means that a safety issue, including the primary safety review, which will be subjected to independent review, should be documented in such a way that another party can review it.

In order to be able to fulfil its duties in the necessary manner, the independent function for safety review should be given a sufficiently independent position, in relation to the parts of the organisation that are responsible for a specific issue. Normally, the independent function should be subordinate only to the highest manager. In order to maintain this independent function, its personnel should not participate in work on analyses or investigations of issues as long as such work is being handled within the responsible organisational parts.

If the operation of a facility is contracted out to a third party in accordance with the Act on Nuclear Activities, the licensee should clarify and report to the Swedish Nuclear Power Inspectorate how the functions of primary safety review as well as independent safety review are allocated between the licensee and the contractor, for the different cases where safety review is to be carried out in accordance with the requirements of these regulations.

Chapter 4, Assessment and Reporting of the Safety of Facilities

Engineered or organisational modifications to a facility that can affect the conditions specified in the safety report as well as essential modifications to the report shall be reviewed in accordance with Chapter 3.

Before the modifications may be introduced, the Swedish Nuclear Power Inspectorate shall be notified and the Inspectorate can decide that additional or other requirements or conditions shall apply with respect to the modifications.

Comment: In this context, engineered modifications are modifications to the design or layout of barriers as well as systems, components and devices which are needed to ensure that the defence-in-depth safety functions perform as intended in the safety report.

Organisational modifications are such changes which are of essential importance for the management and control of operation, maintenance, handling of nuclear material and nuclear waste, work on safety and quality assurance as well as emergency preparedness.

Essential modifications to the safety report are e.g. changes in the design or functional requirements, changes in the principles for operability checks and changes resulting from safety analyses.

In this context, it should be observed that changes in the software used in control equipment which have an effect on a safety function are also to be considered to be modifications to the facility.

The Swedish Nuclear Power Inspectorate should be notified of any modifications in as good time as is possible and reasonable, taking into account the nature of the matter.

4. LICENSEE REQUIREMENTS AND REVIEW

Safety requirements

To exemplify safety requirements applicable for a nuclear power unit, the requirements for Forsmark unit 3 are used. These requirements are documented in chapter four of the safety analysis report.

General safety requirements

With few and documented exceptions the US NRC General Design Criteria (10CFR50 App. A) are applied. With documented exceptions US NRC Regulatory Guides, division 1, which was issued before 1985, are also applied. Some Regulatory Guides in division 1 who have been issued after 1985 are added to the requirement chapter in the FSAR.

With documented exceptions and interpretations, a selected number of US standards and guides are applied, e.g.:

- ANSI/ANS 52.1, 58.9 and others.

- IEEE 278, 323, 336, 344, 352, 379, 384, 730.1 and others.
- IEC 880, 987 and others.
- ISO 9000-3 and others.

Specific safety requirements

The purpose of specific requirements on software based systems is to reduce the probability of Common Cause Failures (CCF). An efficient approach to reduce the probability for CCF is to apply comprehensive verification and validation (V&V) activities and to use good design methods and routines through out the whole life cycle of a software based project, i.e. during all phases, from requirement engineering to operation and maintenance and modifications. Specific safety requirements, depending on safety categorisation are documented in appendix 1.

In addition to the specific requirements the following general requirements shall be applied:
- New equipment and functions shall at least fulfil the same safety requirement level as was required for the old, conventional equipment and functions.
- General safety requirements shall be applied when applicable.
- The same requirements apply for the hardware as for conventional equipment and functions used for the same application.

Detailed design requirements are stated in the document: *Technical Requirements for Electrical Equipment*, TBE.

Safety case analysis

A proposal for a plant modification is basically documented in two documents:
- Plant Modification Proposal
- Plant Modification Implementation Plan

Both documents contain a safety requirement specification as well as a safety case analysis. Both documents are, after review and approval and, in case of a category A modification, submitted to the authority as a notification.

Safety review

The primary safety review of a plant modification proposal and plant modification implementation plan is performed by the operations department at the unit concerned by the modification. In addition, the quality and safety department also reviews the modification package. This department is organised directly under the Forsmark CEO and consequently not involved in the preparation or execution of the modification. However, this second review is not a repeat of the first one, but more a judgement as to whether the issue has been treated in a satisfactory way from a safety point of view. Consequently, focus is on the analyses that the conclusions are based on and whether these analyses have been performed with enough depth and sufficient professional quality. The safety review of category A modification is concluded with a submission to the safety committee.

5. HARMONISATION WORK

Both the Swedish regulator, SKI, and the Swedish utilities are actively participating in several organisations, on different levels, in the international harmonisation works.

Regulatory activities

- European Commission's Advisory Experts Group, The Nuclear Regulator's Working Group, Task Force on Safety Critical Software, NRWG TF. The task force published a report in May 2000 on "Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors. The Task Force will continue to work with harmonisation issues.
- Western European Nuclear Regulators Association, WENRA. The nuclear safety authorities in the Western Europe decided in November 1999 to investigate major differences in nuclear safety in the countries belonging to the European Union and suggest harmonisation measures. A pilot study is ongoing in order to establish a screening methodology, able to compare existing, by law binding requirements, and how they are applied. To begin with, four areas were selected: Safety management, design, operation and safety verification. After the screening, a reference level was selected and the deviation for each country was noted. The reference was selected to correspond to the upper quarter of the requirement level of all involved countries. The pilot study shows that a structured and useful method has been developed. The pilot study is expected to be finalised in the middle of 2002.
- OECD/NEA Common Nuclear Regulators Activity, CNRA.

Utility activities

- European Utility Requirements, EUR. The main objective of the EUR organisation is to produce a common set of utility requirements, endorsed by the major European electricity producers for the next generation of LWR nuclear power plants. EUR volume 2, chapter 2.10 presents the general design and architecture criteria that shall be applicable to all instrument & control (I&C) and man-machine interface of an advanced LWR plant.
- IEC, for example TC45 and IAEA, for example TWG-NPPCI. The Swedish utilities are actively participating in the standardisation work that is performed within the International Electrotechnical Commission, IEC, as well as in the different technical committees set up by IAEA. This participation facilitates harmonisation and increases the understanding of the need to standardisation.

Appendix 1, Safety Requirements for software based equipment and functions

Table 1. Requirements on usage of COTS and system requirements for specific application software

Class	Components, non complex COTS systems	COTS	Systems requiring a specific application software
1E	A quality system that fulfils the requirements of ISO 9000-3. Deviations shall be approved. Operating experience requirements: >1000 components in operation > 1 year. Failure handling programme in operation.	Software design according to the principles in IEC 880 or IEEE 730.1 Deviations shall be approved. Operating experience requirements: >10 applications in operation. Failure handling programme in operation.	Software design according to the principles in IEC 880 or IEEE 730.1 Deviations shall be approved. Operating experience requirements: Not applicable. Failure handling programme in operation.
2E	A quality system that fulfils the requirements of ISO 9000-3. Deviations shall be approved.	Software design according to the principles given by ISO 9000-3. Deviations shall be approved.	Software design according to the principles given by ISO 9000-3. Deviations shall be approved.
3E	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.

Table 2 Requirements on programme execution and fail-safe operation.

Class	Components, non complex COTS systems	COTS	Systems requiring a specific application software
1E	The programme execution shall be load independent. This requirement shall be verified by tests. Fail-safe operation when applicable.	The programme execution shall be load independent. The fulfilment of this requirement shall be demonstrated by deterministic methods and verified by tests. Fail-safe operation.	The programme execution shall be load independent. The fulfilment of this requirement shall be demonstrated by deterministic methods and verified by tests. Fail-safe operation.
2E	The programme execution shall be load independent. This requirement shall, if possible, be verified by tests. Fail-safe operation when applicable.	The programme execution shall be load independent. This requirement shall, if possible, be verified by tests. Fail-safe operation.	The programme execution shall be load independent. The fulfilment of this requirement shall be demonstrated by deterministic methods and verified by tests. Fail-safe operation.
3E	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.

Table 3 Specific requirements on the design of computer memories

Class	Components, non complex COTS systems	COTS	Systems requiring a specific application software
1E	Programme and data shall be stored in non-volatile memories (PROM or EPROM) Data may be stored in volatile and changeable memories if the storage can be supervised and fail-safe.	Programme and data shall be stored in non-volatile memories (PROM or EPROM) Data may be stored in volatile and changeable memories if the storage can be supervised and fail-safe.	Programme and data shall be stored in non-volatile memories (PROM or EPROM) Data may be stored in volatile and changeable memories if the storage can be supervised and fail-safe.
2E	Programme and data shall be stored in non-volatile memories (PROM or EPROM) Data may be stored in volatile and changeable memories if the storage can be supervised and fail-safe.	For systems and functions of importance for production, the same requirements as for 1E shall be applied. For other systems and functions pro-gramme, data etc. may be stored in volatile and changeable memories that are fail-safe.	Programme, data etc. shall be stored in volatile and changeable memories that are fail-safe.
3E	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.	If motivated, the same requirements as for 2E shall be applied. In other cases, the requirements shall be adjusted to what is appropriate for the application.

BIBLIOGRAPHY TO APPENDIX A.8

Ds 2001:41 Sweden's second national report under the Convention on Nuclear Safety.

SKIFS 1998:1 The Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities; Decided on August 11, 1998. (English version)

FKA-I-824 Forsmark – Safety review (procedure, only in Swedish).

FKA-I-259 Forsmark – Procedure on plant modifications (only in Swedish).

FKA-I-274 Forsmark – Ordering of plant modifications (procedure, only in Swedish).

FKA-I-261 Forsmark – Procedure on the performance of plant modifications (only in Swedish).

APPENDIX A.9.

UKRAINE, COUNTRY REPORT

(provided by M. Yastrebenetsky/Ukraine State Scientific Technical Center on Nuclear and Radiation Safety)

1. INTRODUCTION

Digital I&C systems are as more and more widely adopted from year in Ukraine instead of analog systems used earlier under modernization of operating NPP as well as under construction of new NPP Rovno 4 and Khmelnitsky 2 .

During last five years a lot of digital systems for all units of VVER-1000 and both units of VVER-440 (e.g. computer information systems, digital regulators, control rod systems, safety parameter display systems) were implemented. Even at Unit 3 of Chernobyl NPP closed in December 2000, some modernization with use of digital systems was carried out two years before the closing.

Systems designed not only (not so much) by Ukrainian manufacturers, but also by manufacturers from other countries (USA, France, Czech Republic, Russia, Germany) are and will be used at Ukrainian NPPs. Wide use of digital systems for NPP safety applications resulted in necessity of creation of standard base and principles of licensing process realization.

2. STANDARD BASE RELATED TO DIGITAL I&C

The USSR standards for NPP I&C which have used in Ukraine earlier, were built upon different principles and had many contradictions (from definitions of main terms to quality and quantity requirements to NPP I&C characteristics). These standards did not account the peculiarities of software based systems and requirements of international standards (for example, these standards did not have the requirements to equipment qualification, software verification and validation).

These lacks were as reasons for elaboration of new Ukrainian standard base on digital I&C. The documents are as a part of Ukrainian nuclear legislation pyramid. It is possible to distinguish three hierarchical levels in this pyramid.

The documents of state governmental authorities (Laws of Ukraine and Ordinances of the Cabinet of Ministers) identifying the order of state safety regulation regarding the area of nuclear power form the top level.

The main ones of them are as the following:

- Law of Ukraine “On Use of Nuclear Power and Radiation Safety” [1];
- Law of Ukraine “ About Permission Activity on Nuclear Energy Utilization”.

According to the [1], the state safety regulation shall provide the following:

- Establishing regulatory criteria and requirements determining conditions of use of nuclear facilities);

- Licensing – granting permission for the activity related to the use of nuclear facilities;

- Supervision -control of over meeting regulatory requirements and conditions of the given permission.

The second level are as the standards and rules elaborated by Ukrainian Nuclear Regulatory Authority NRA (a new name since 2000 – State Nuclear Regulatory Committee of Ukraine).

These documents contain general positions as per NPP safety assurance including related to I&C important to safety. The most important document (from I&C) in this level is as document NP 306.1.02/1.034-200. "General Provisions of Nuclear Power Plant Safety Assurance" [2].

The third level contains NRA documents related to different types of NPP equipment and tasks. New documents related digital I&C are belonged to this level. In principle, different approaches were possible for Ukraine during the establishment of these documents for I&C:

- to accept the safety regulation documents that are in force in any state with the developed regulatory frame work (USA, Germany, France, Russia) as regulatory requirements;

- without elaborating of own requirements to use the requirements of international safety standards and guidelines developed by IAEA, IEC, ISO as regulatory requirements;

- to formulate own regulatory requirements taking into consideration national and international experience in the regulation and safety assessment, as well as available scientific and economical possibilities for providing the safety of Ukraine NPP.

The NRA approved the last approach since:

- the own system of regulation documents on nuclear safety has been already formed in Ukraine. New documents approved by NRA should be put in this system;
- I&C which are implemented in Ukrainian NPP have been developed not only by Ukrainian organizations, but also by many other companies, each of them applies the regulatory framework of its country. It is evident that regulatory requirements of Ukraine should be unique for all these systems;
- countries with the different economical development have different possibilities for assuring and confirming the safety; this essentially affects on the level of regulatory requirements.

We give only one example confirming the correctness of the accepted approach. The classification of I&C and their components by safety is applied in Ukraine. This classification complies with general classification of NPP systems and elements given in [2], and is closed to IAEA classification [3].

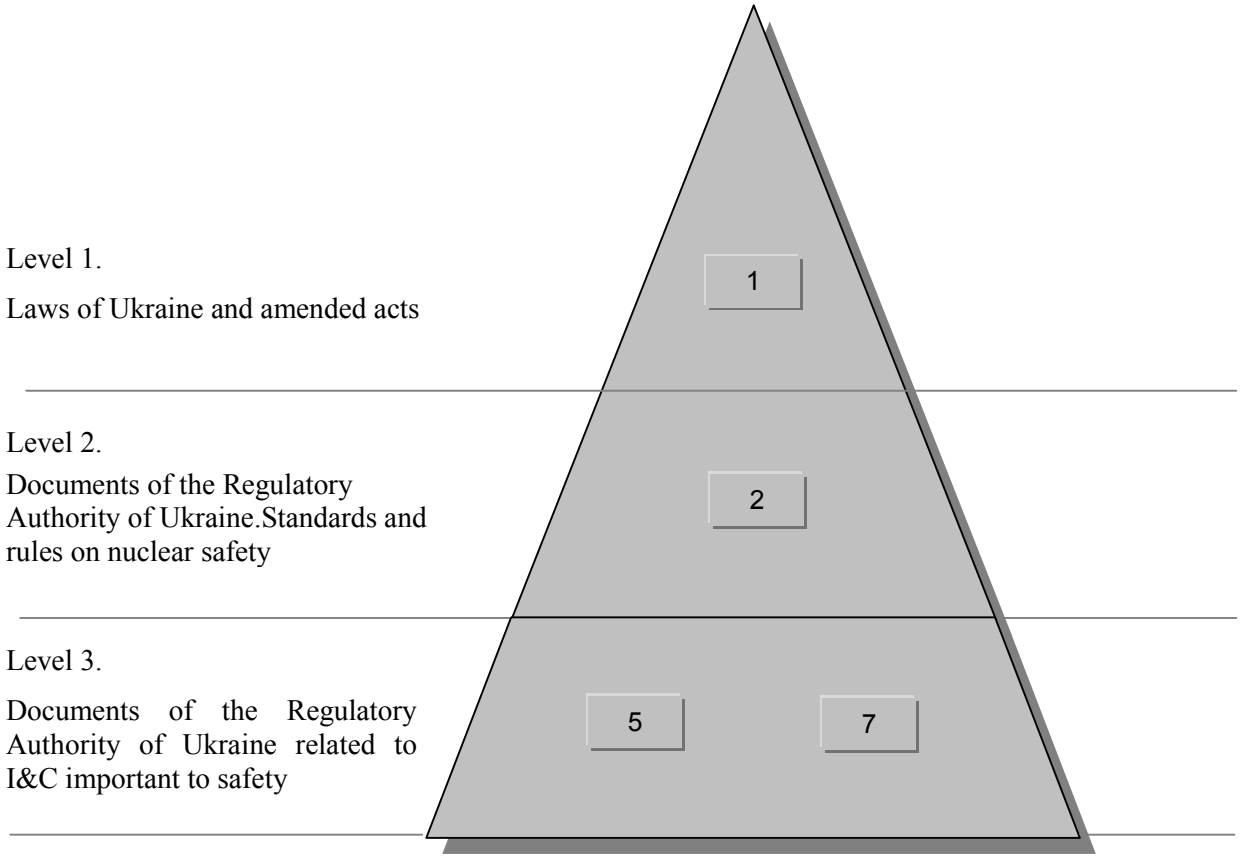


FIG. A9.1. Pyramid of Regulation Documents on Nuclear Safety in Force in Ukraine.

At the same time, in IEC standard [4] four safety categories have been established. In spite of the progress of the proposed classification, its application can not be recommended for the application presently in Ukraine not only due to the difference [2] but also because it would require the revision of the most regulatory, design, operation and other documents that applied accepted previously classification.

According to [1], one of these documents [5,6] is related to regulatory criteria, the second [7,8] – to licensing process. The peculiarities of standard [5]:

- covers new, reconstructed and modernized I&C important to safety and their components: hardware and software;
- does not contradict the basic regulation documents on nuclear safety that are in force in Ukraine [1, 2], standards related to industrial control systems, etc.;
- as much as possible takes into consideration the requirements of international safety standards and guidelines [3, 4, 9, 10, etc.] which are absent in the regulation documents that are in force in Ukraine (not only the acting documents but drafts of IAEA documents [11]);
- applies the experience of safety regulation reflected in the national standards and rules of advanced countries.

Structure of Standard [5] is shown on figure 2.

Content of Standard [7] is as the following:

- General Provisions.
- Terms and Definitions.
- List of the documents used for I&C safety assessment:
  - NPP Technical Decisions about modernization;
  - System Terms and References;
  - V&V Plan and Report;
  - Safety Analysis Report
  - Site Acceptance Test Program, methodic, report, etc.
- Criteria for assessment.
- Rules for safety assessment during expertise.

3. LICENSING PROCESS

Table 1 shows a procedure of licensing process during I&C modernization: connection between list of documents, which delivers to NRA, the list of expert reviews and NRA decisions (license). The expert reviews were fulfilled with use of databases (figure 3).

Database "Regulatory requirements" contains requirements from different types of documents:

- standards and rules, acted in Ukraine;
- international organization (IAEA, IEC, ISO, etc.);
- national standards which are de-facto international (f.e. IEEE – USA);
- national standards of countries-designers of I&C for Ukraine.

The last type of documents can be used if I&C was designed by foreign country – designer standards and we have to evaluate if differences between country – designer and Ukrainian standard may lead to safety violations (the most simple example of this: differences between limits of power supply deviations).

The choosing of requirements depends on safety classification, purpose of system, nature of assigned functions. Database "I&C expert reviews" contains full texts of 117 reviews with descriptions of 29 modernized systems safety assessments. These reviews were fulfilled for 1996-2002 for following systems:

- group and individual control rod system (Scoda – Czech Republic);
- computer information system (SYSECA – France);
- computer information system (Westinghouse – USA);
- safety parameters display system (Westinghouse – USA);
- refueling machine control system (Odessa Polytechnic University – Ukraine);
- refueling machine control system (Hanz – Hungary);
- computer system from machine room control (Shevchenko Plant – Ukraine);

- computer regulators of 1-st circuit (Shevchenko Plant – Ukraine);
- steam generator level and feedwater control system (WESE – Belgium);
- protection system, neutron flux monitoring system (Siemens – Germany);
- in-core reactor monitoring system (Impuls – Ukraine);
- power regulator (Khartron – Ukraine).

Database “Modernization of NPP I&C” contains an information about modernized systems which have been implemented or are under implementation now. This database is limited for I&C of VVER-1000 and VVER-440 units which used in Ukraine, Russia, Bulgaria and the other countries. This database contains the information about type of modernized and old system, designer, year of modernization, volume of modernization, main technical characteristics, etc.

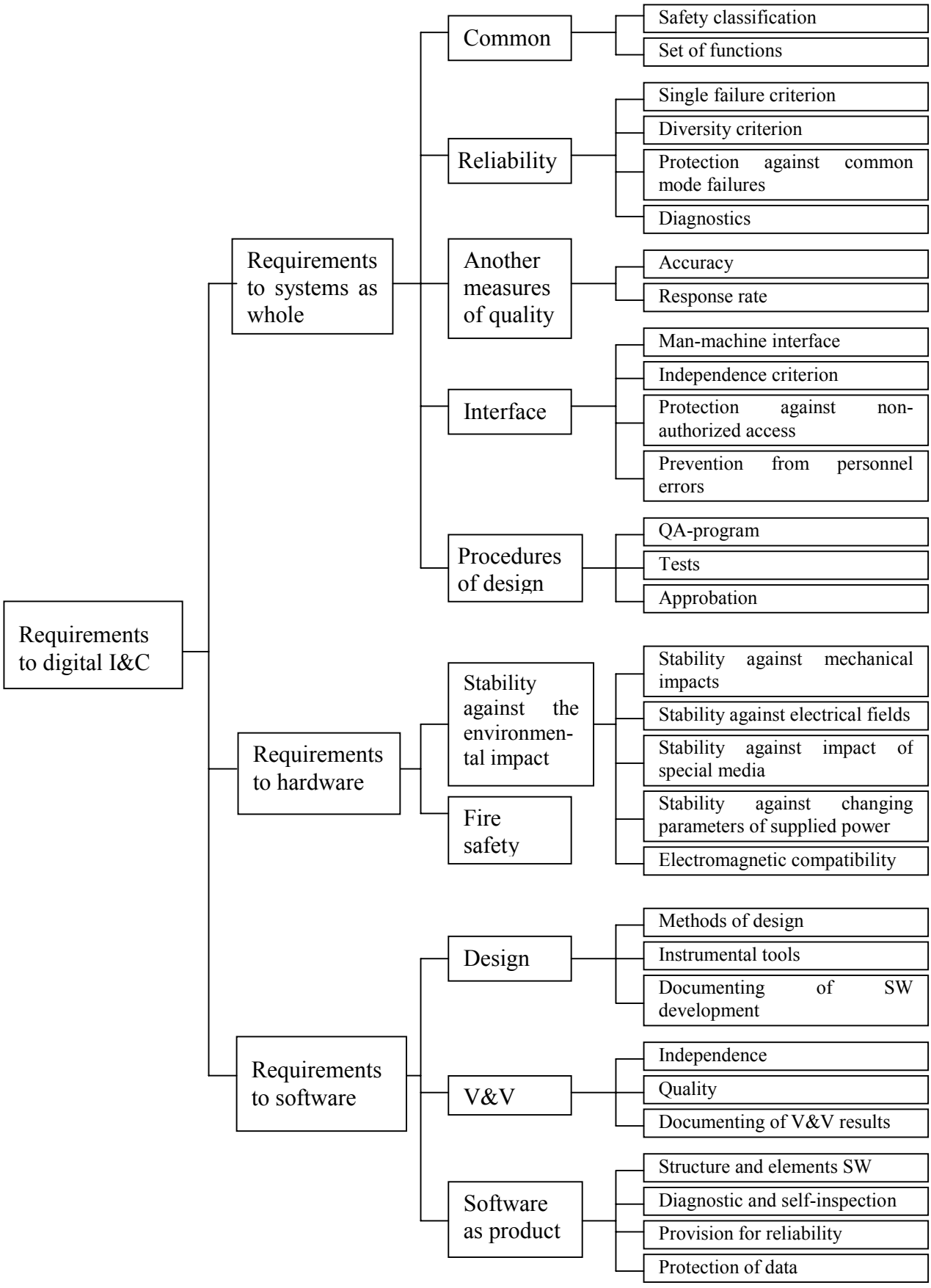


FIG . A9.2. Structure of standard "Requirements of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety on NPP".

Table 1. Steps of Digital I&C licensing

Documents basing the safety and represented by operation organization into NRA	**Expert review with safety assessment results**	**Document of NRA**
NPP Conceptual Technical Decision on I&C modernization	Expert review of Conceptual Technical Decision along with project of licensing plan	Agreement of Decision Approval of licensing plan.
Terms of References	Expert review	Agreement of Terms of References
Quality Assurance Program		
Software Verification Plan and Report	Expert review	Agreement of license on erection
Validation Plan and Report	Expert review	
Preliminary Safety Analysis Report	Expert review	
Program and Methods of Site Acceptance Tests (SAT)	Expert review	Agreement of decision on I&C System Commissioning
Report as per Results of SAT		
Final Safety Analysis Report	Expert review	

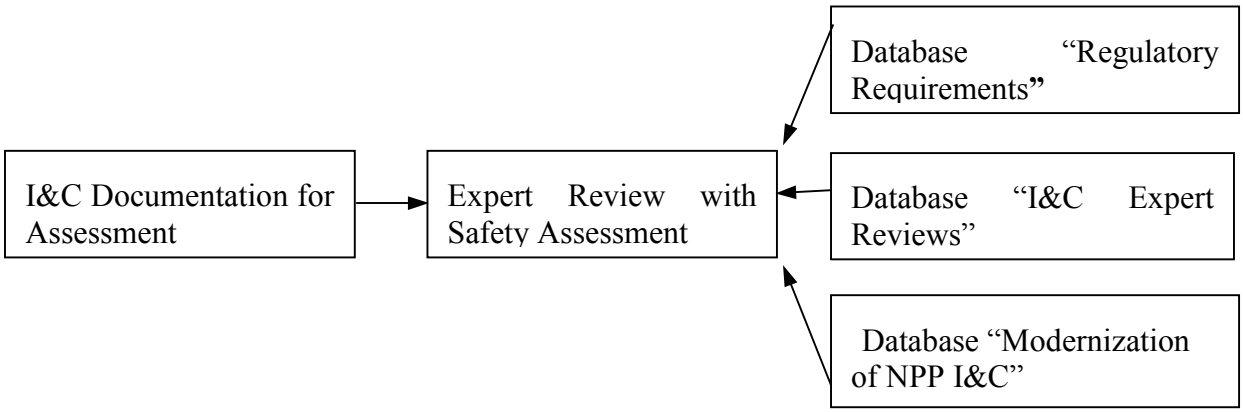


FIG. A9.3. Database for expert reviews elaboration of digital I&C.

REFERENCES TO APPENDIX A.9

[1] Law of Ukraine “On use of Nuclear Power and Radiation Safety”.

[2] NP 306.1.02/1.034-2000. General Provisions of Nuclear Power Plant Safety Assurance.

[3] IAEA 50-SG-D3. Protective Systems and Related Features in Nuclear Power plants. Safety Guideline, 1982.

[4] IEC 61226. Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Classification, 1993.

[5] NP 306.5.02/3-2000. Requirements of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety on NPP. Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

[6] M. Yastrebenetsky, Yu. Rozen, V. Vasilchenko & S. Vilkomir. Elaboration of Common Regulatory Requirements on Modernized NPP Instrumentation and Control System Important to Safety. Foresight and Precaution. A. A. Balkema, Rotterdam, 2000, p. 813-817.

[7] NP 306.7.02/2.041-2000. Methods of Assessments of Compliance of I&C Systems with Safety Requirements. Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

[8] M. Yastrebenetsky. Safety Assessment of NPP Instrumentation and Control Systems. Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC & HMIT 2000). American Nuclear Society, 2000, Washington, DC.

[9] IAEA 50-SO-D8. Safety-Related Instrumentation and Control Systems for Nuclear Power Plant Safety Assurance. Safety Guideline, 1985.

[10] IEC 60880. Software for Computers important to safety in NPP's.

[11] IAEA Safety Standards. Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Draft Safety Guide. ID DS 252 IAEA, 2000.

APPENDICES B

APPENDIX B.1.

ADVANCED LIGHT WATER REACTOR UTILITY REQUIREMENTS DOCUMENT: OVERVIEW OF ITS DEVELOPMENT, MAIN FEATURES, AND APPLICATION

(provided by J. Naser, EPRI, USA)

U.S. utilities, with extensive support and participation from several international companies, as well as the close cooperation of the U.S. Department of Energy (DOE), led an industry-wide effort to establish a technical foundation for designing the next generation of light water reactors (LWRs), referred to as Advanced Light Water Reactors (ALWRs). The cornerstone of this effort was the utility design requirements, the ALWR Utility Requirements Document (URD).

ALWR requirements are driven by utilities, but with broad industry participation, including U.S. nuclear steam supply vendors, as well as engineering service, consulting, architect-engineer, and construction companies. Thus there was essentially a consensus of the industry as to those features to be sought in the next generation of plants, based on the information and lessons learned from over 35 years of operating over 100 LWRs in the U. S. and many more internationally.

The ALWR Utility Requirements Document addresses the entire plant, including nuclear steam supply system and balance of plant. The requirements intend to provide improved and standardized versions of ALWRs, which eliminate most of the problems and inefficiencies associated with some of the existing designs; assure a simpler, more forgiving plant design which is excellent in all respects, including safety, performance, constructibility, and economics.

The U. S. Nuclear Regulatory Commission (NRC) is directly involved with the URD and has published a Safety Evaluation Report on the requirements for each type of ALWR. Through the NRC review, the URD supports improved stability in the regulatory basis for ALWRs by including agreements on outstanding licensing and severe accident issues.

Looking forward, the URD provides a set of utility technical requirements which can be used in developing an ALWR investor bid package for detailed design, licensing and construction, and which provide a basis for investor confidence in implementing an ALWR.

1. INTRODUCTION AND BACKGROUND

The Electric Power Research Institute (EPRI) began the activity to develop a new generation of LWRs in 1983 through the establishment of preferences and prerequisites of utility executives for ordering new nuclear power plants. Utility executives indicated that new plants must be safer and simpler and must have greater design margins. They also supported making improvements to established LWR technology, rather than developing new reactor concepts requiring prototype demonstrations. Further, they wanted the option to build midsize nuclear plants in addition to large sized plants. Midsize plants could better support the demands of slower load growth, and would more readily accommodate the introduction of safety features

that rely on natural forces, thereby providing additional opportunity to simplify plant design and operation.

In response to industry guidelines, EPRI initiated the ALWR design effort in 1985 beginning development of the ALWR Utility Requirements Document (URD)[1]. In addition to providing a comprehensive set of utility design requirements, the document was to address over 700 regulatory issues required to be resolved for future designs by the U.S. Nuclear Regulatory Commission (NRC) . The first three volumes in the URD were completed in 1990 and contain more than 14,000 detailed requirements for ALWR designs. The NRC published their Safety Evaluation Report (SER) [2] in 1992 and 1994 detailing their review of the URD.

Work on the URD provided a foundation for follow-on-design programs, as well as the development of an integrated, industry-wide plan for and commitment to the resolution of challenges to building new nuclear power plants. The goal of the overall program is described in the Strategic Plan for Building New Nuclear Power Plants [3], published by the Nuclear Energy Institute (NEI) Executive Committee to resolve the full spectrum of issues, technical and institutional, in an integrated and coordinated way.

The remaining sections of this paper describe the development, organization and content, and use of the URD in ALWR implementation. Much of the content of this paper is from Volume I of the URD.

2. DEVELOPMENT OF THE REQUIREMENTS DOCUMENT

Overall direction in developing the URD was provided by the ALWR Utility Steering Committee (USC) consisting of senior representatives from approximately twenty U.S. and foreign utilities. EPRI personnel acted as staff to the USC. EPRI also established contracts with U.S. nuclear steam supply system vendors, as well as engineering service, consulting, architect-engineer, and construction companies. As a result, the ALWR requirements were driven by utilities, but have also have had the benefit of participation of a broad range of industry participants. Thus, the requirements are essentially a consensus of the industry as to those features which should be sought in the next generation of plants.

The USC established policy statements in key areas which were central to achievement of program objectives and which have broad, fundamental influence on plant design requirements. These policy areas tend to be pervasive ones which the utility sponsors consider important to correcting problems (e.g., plant simplification) in existing plants or to be ones which explain fundamental ALWR guiding principles (e.g., use of proven technology). The policy statements are not considered design requirements by themselves, but rather influence or form the foundation for a set of requirements. The fourteen policy statements are discussed further in Section 4.

The main focus of the requirements and commensurate level of detail is on areas of improvement needed to achieve an excellent power plant. Considering the policy statements as well as the scope and focus of the requirements, the URD was organized into volumes, based on plant designs, and chapters based on plant systems and topics.

The development of individual chapters followed an iterative, consensus building approach. Initial chapter drafts were developed by a selected team of engineers from among ALWR contractors. Chapter Managers were selected to lead the development effort and consensus building process. Periodic meetings with representatives from contractor organizations were held to review and resolve comments on chapter drafts. A formal database of comments and

their resolution supported the drafting process. Periodic meetings were held to appraise the USC of progress and key issues associated with the development of each chapter. When chapter drafts achieved sufficient maturity and all comments were dispositioned, they were provided to the USC for review and approval. In September, 1990, after about five years of development, the first complete revision of the URD was sent to the NRC for their review.

The development of the URD was an unprecedented effort by utilities to provide, at new levels of comprehensiveness and clarity, their desires for future nuclear plant designs. The URD development process presented an opportunity for utilities to consider approaches to most effectively communicate to designers. As the process evolved, preferences regarding the format, level of detail, and style for writing requirements became clear as did the need to tailor requirements based on the characteristics of the subject matter. The specificity and comprehensiveness employed for developing the requirements varied depending on the operational feedback and improvements desired. Considerable emphasis is placed on the incorporation of human factors in the design process and improvements in the man-machine interface in general, and specifically the main control room.

Once the first version of the URD was produced, a means of maintaining and updating the document was required. A formal process was established to request changes to the URD, to have changes reviewed by all interested participants, to obtain approval of changes by the USC, and finally, to implement changes in revisions to the URD.

Changes to the requirements have been processed based on review comments from the NRC, and, more recently, on feedback from the ALWR design projects. For example, the latest revision of the URD has greatly benefited from completed ABWR first-of-a-kind engineering (FOAKE) as well as AP600 design certification and FOAKE efforts. Figure I shows the model presently implemented between EPRI, representing the utilities, and the designers in developing ALWR designs. The feedback loops show that changes to the requirements or to the design may be needed to assure conformance between requirements and design.

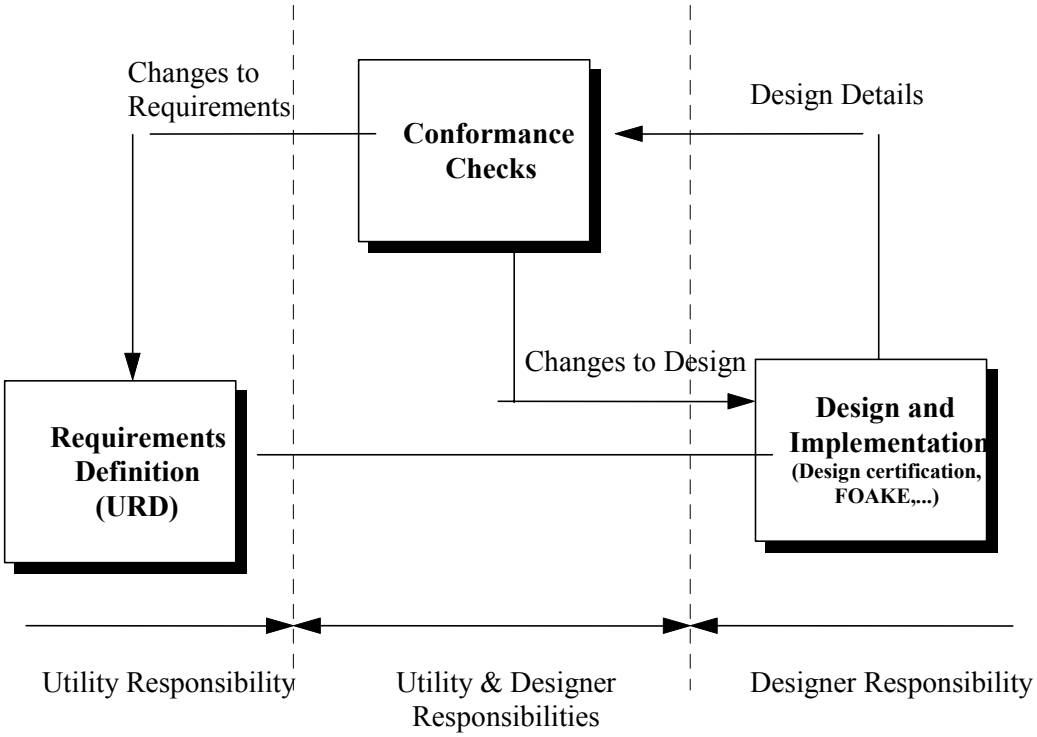


FIG. B1.1. ALWR utility requirements document in a design process.

To date there have been eight revisions to the URD incorporating over 600 changes. While there has been a sizable number of updates to the URD, it is clear that the URD has demonstrated its value in focusing and directing design processes toward the needs and desires of potential owners and operators.

3. ORGANIZATION OF THE REQUIREMENTS DOCUMENT

A systematic approach has been taken in developing and organizing the requirements. The URD covers the entire plant up to the grid interface. It therefore is the basis for an integrated plant design, i.e., nuclear steam supply system and balance of plant, and it emphasizes those areas which are most important to the objective of achieving an ALWR which is excellent with respect to safety, performance, constructibility, and economics. The document applies to both Pressurized Water Reactors (PWRs) and Boiling Water Reactors (BWRs). An overall illustration of the structure of the document is provided in Figure II.

Volume 1 of the document defines ALWR Program policy and summarizes top-tier design requirements. The policy statements provide utility positions on key aspects of design, development, and ALWR Program implementation. The top-tier design requirements are key elements in meeting ALWR Program objectives to make available a viable nuclear power generation option in the future. They also form the basis for developing detailed requirements in subsequent volumes for specific plant concepts.

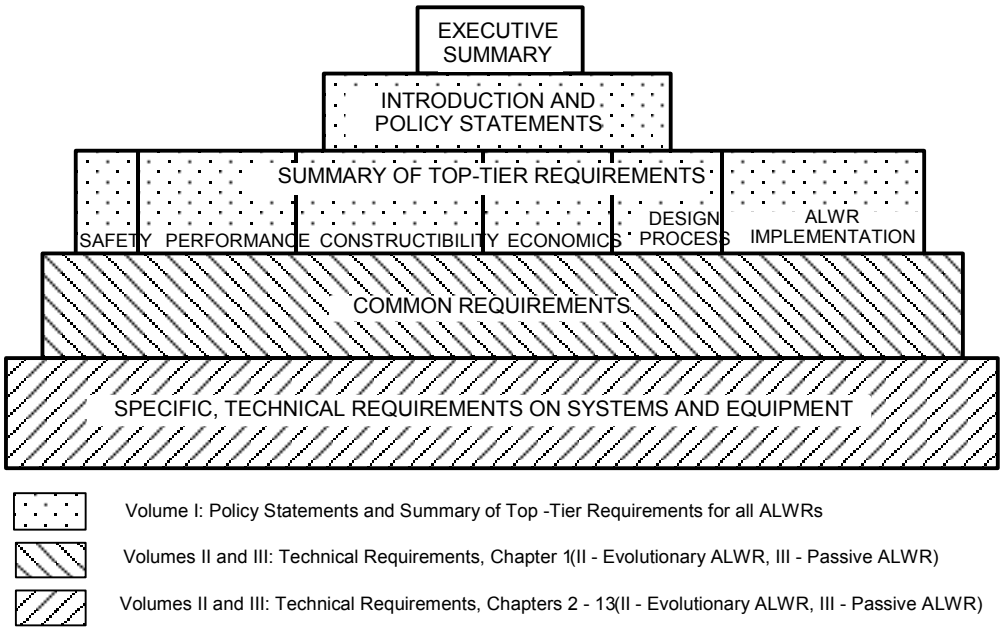


FIG. B1.2. ALWR utility requirements document organization.

Volume 1 is written in a narrative format (versus the requirements — rationale format used in Volumes II and III as described below) in order to present the policies and top-tier requirements in a more compact manner. Also included in Volume I is a section which defines ALWR cost goals to assure that the ALWR is economically competitive with other generation alternatives. Finally, a section is included on plausible scenarios for ALWR implementation, including certification, design, and construction.

Volumes II and III of the URD contain the complete set (top-tier and detailed) of design requirements for the Evolutionary and Passive ALWRs, respectively. Chapter 1 of each volume defines common requirements applicable to a number of plant systems. These requirements are in one chapter to avoid repetition in the subsequent chapters. Chapters 2 through 13 of each volume have been organized by groups of systems to cover the entire nuclear plant. URD chapter titles are shown below in Table 1.

Table B1.1. ALWR Utility Requirements Document Chapters

Chapter	Title	Chapter	Title
1	Overall Requirements	5	Engineered Safety Systems
1A	PRA Key Assumptions and Groundrules	6	Building Design and Arrangement
1B	Licensing and Regulatory Requirements and Guidance	7	Fueling and Refueling
		8	Plant Cooling Water Systems
1C	Cost Estimating Groundrules	9	Site Support Systems
2	Power Generation Systems	10	Man-Machine Interface Systems
3	Reactor Coolant System and Reactor Non-Safety Auxiliary Systems	11	Electric Power Systems
		12	Radioactive Waste Processing Systems
4	Reactor Systems	13	Turbine Generator Systems

3.1 Requirement/engineering rationale approach

The design requirements specified in the URD are organized in a side-by-side format which provides an engineering rationale for each requirement. The requirements define utility positions on the means for resolving problems in design, construction, and operation of current plants and for meeting the ALWR Program objectives. The rationale presents the basis for the requirement and provides later users of the document a better understanding of the requirement and its intent.

Volume I and introductions to various sections of Volumes II and III include narrative text that is not in the side-by-side format. This narrative text typically states ALWR policy or necessary background. Although not strictly considered to be plant design requirements as the side-by-side format, narrative text provides understanding of ALWR policy and perspective on program background or section scope.

3.2 Explanation of requirement terminology

The URD requirements are mandatory features and attributes of ALWR designs which are necessary to satisfy the Plant Owner that the plant will be excellent in all aspects. By definition then, requirements are directed at the plant design team, i.e., the Plant Designer, and compliance with them should be demonstrable. Requirements are intended to be challenging, yet achievable.

It is the intent of the ALWR Program to provide a set of compatible requirements which result in an integrated design which meets overall ALWR program objectives. The URD is not a set of requirements to be selected and chosen from, but rather to be invoked as an integrated set of requirements which establish the plant design basis for the Plant Designer.

There are a number of very desirable plant characteristics which are established as design requirements but are in areas which pertain to factors beyond the Plant Designer's complete control, such as volume of radioactive waste produced, plant construction schedule, and plant availability. In these cases, the intent is to require the Plant Designer to develop and demonstrate a plant design for which the stated characteristic can be achieved by a competent and professional constructor and owner/operator organization.

4. ALWR POLICIES AND TOP LEVEL REQUIREMENTS

The ALWR Program has formulated fourteen policies in order to provide guidance for overall URD development, and to provide guidance to the Plant Designer in applying the requirements. While not design requirements themselves, the policies cover fundamental ALWR principles which have a broad influence on the design requirements. Key policy statements are shown below in Table 2.

Table B1.2. Summary of ALWR Utility Requirements Policies

Simplification	Simplification is fundamental to ALWR success. Simplification opportunities are to be pursued with very high priority and assigned greater importance in design decisions than has been done in recent, operating plants; simplification is to be assessed primarily from the standpoint of the plant operator.
Design Margin	Like simplicity, design margin is of fundamental importance and is to be pursued with very high priority. It will be assigned greater importance in design decisions than has been done in recent, operating plants. Design margins which go beyond regulatory requirements are not to be traded off or eroded for regulatory purposes.
Human Factors	Human factors considerations incorporated into every step of the ALWR design process. Significant improvements will be made in the main control room design.
Safety	Excellence in safety for protection of the public, on-site personnel safety, and investment protection. Places primary emphasis on accident prevention as well as significant additional emphasis on mitigation. Containment performance during severe accidents is evaluated to assure that adequate containment margin exists.
Design Basis Versus Safety Margin	ALWR designs will include both safety design and safety margin requirements. Safety design requirements (Licensing Design Basis) are necessary to meet the NRC's regulations with conservative, licensing-based methods. Safety margin requirements (Safety Margin Basis) are Plant Owner-initiated features which address investment protection and severe accidents on a best estimate basis.
Regulatory Stabilization	ALWR Licensability is to be assured by resolving licensing issues, appropriately updating regulatory requirements, establishing acceptable severe accident provisions, and achieving a design consistent with regulatory requirements
Standardization	The ALWR utility requirements will form the technical foundation which leads the way to standardized, certified ALWR plant designs.
Proven Technology	Employed throughout ALWR designs to minimize investment risk, control costs, take advantage of existing operating experience, and assure that a plant prototype is not required; proven technology is successful and clear demonstration in LWRs or other applicable industries such as fossil power and process industries.
Maintainability	Ease of maintenance to reduce operations and maintenance costs, reduce occupational exposure, and to facilitate repair and replacement of equipment
Constructibility	The ALWR construction schedule will be substantially improved over existing plants and must provide a basis for investor confidence through use of a design-for-construction approach, and completed engineering prior to initiation of construction.
Quality Assurance	The responsibility for high quality design and construction work rests with the line management and personnel of the Plant Designer and Plant Constructor teams.
Economics	ALWR plants will be designed to have projected busbar costs with a sufficient cost advantage over competing baseload electricity generation technologies to offset higher capital investment risk associated with nuclear plant utilization.
Sabotage Protection	Inherent resistance to sabotage plus protection by plant security and integration of plant arrangements and system configuration with plant security design.
Good Neighbor	The ALWR plant will be designed to be a good neighbor to its surrounding environment and population by minimizing radioactive and chemical releases.

4.1 ALWR top-tier design requirements

A brief summary of top-tier utility design requirements is provided in Table 3; categorized by major functions, including safety and investment protection, performance, and design process and constructibility. There is also a set of general utility design requirements, such as simplification and proven technology, which apply broadly to the ALWR design, and set of economic goals for the ALWR program. These requirements reflect the ALWR Program policies described above and form the basis for developing detailed system design requirements for specific ALWR concepts.

Table B1.3. Summary of Top-Tier ALWR Plant Design Requirements

GENERAL UTILITY DESIGN REQUIREMENTS	
Plant type and size	PWR or BWR, applicable to a range of sizes up to 1350 MW(e) • Reference size for Evolutionary ALWR: 1200–1300 MW(e) per unit • Reference size for Passive ALWR: 600 MW(e) per unit
Safety system concept	• Evolutionary ALWR - simplified, improved active systems • Passive ALWR - passive systems; no safety-related bulk ac power
Plant design life	60 years
Design philosophy	Simple, rugged, high design margin, based on proven technology; no power plant prototype required.
Plant siting envelope	Most available sites in U.S.; 0.3g Safe Shutdown Earthquake (SSE)
SAFETY AND INVESTMENT PROTECTION	
Accident resistance	Design features to minimize initiating event occurrence and severity : • Fuel thermal margin $\geq$ 15% • Slower plant response to upset conditions through features such as increased coolant inventory.
Core damage prevention	Design features to prevent initiating events from evolving to core damage.
• Core damage frequency	Demonstrate by PRA that core damage frequency < 10^{-5} per reactor year.
• LOCA protection	No fuel damage for up to a 6-inch break
• Station blackout coping	8 hours minimum coping time for core cooling (indefinite for Passive ALWR)
Mitigation	
• Severe accident risk	PRA whole body dose less than 25 rem at the site boundary for severe accidents with cumulative frequency greater than 10^{-6} per reactor year.
• Containment Design	Large, rugged containment building with design pressure based on Licensing Design Basis pipe break.
• Containment Margin	Margin in containment design is sufficient to maintain containment integrity and low leakage during severe accident.
• Licensing source term	Similar in concept to existing Reg. Guide, TID 14844 approach, but more technically correct release fractions, release timing, and chemical form.
PERFORMANCE	
Design availability	87%
Refueling interval	24-month capability
Unplanned auto scrams	Less than 1/year
Maneuvering	Daily load follow
Load rejection	Loss of load without reactor or turbine trip for PWR (BWR from 40% power).
Operability and maintainability	
• Design for operation	Operability features designed into plant, such as: forgiving plant response for operators, design margin, and operator environment
• Design for maintenance	Maintainability features designed-in, such as: standardization of components, equipment design for minimal maintenance needs, provision of adequate access, improved working conditions , and ready access to equipment.
• Equipment replacement	Facilitate replacement of components, including steam generators.
Man-Machine Interface	
• Instrumentation and control systems	Advanced technology, including software based systems, multiplexing, alarm prioritization, fault tolerance, and automatic testing.
• Operations simplicity	Single operator able to control plant during normal power operation.

DESIGN PROCESS AND CONSTRUCTIBILITY

Total time from owner commitment to construct to commercial operation	1300 MW(e) evolutionary plant designed for 72 months or less 600 MW(e) passive plant designed for 60 months or less
Design status at time of initiation of construction	90% complete
Design and plan for construction	Design for simplicity and modularization to facilitate construction; develop an integrated construction plan through Plant Owner acceptance.
Design process	
• Design integration	Manage and execute design as a single, integrated process.
• Configuration control	Comprehensive system to control plant design basis.
• Information management	Computerized system to generate and utilize integrated plant information during design, construction, and operation

5. ROLE OF REQUIREMENTS IN ALWR IMPLEMENTATION

There are three primary roles of the ALWR design requirements in ALWR implementation as illustrated in Figure 3.

5.1 Establishing a stabilized regulatory basis

The ALWR requirements will help establish a stabilized regulatory basis through actions in four areas: (1) licensing issue resolution, (2) regulatory requirement optimization, (3) establishing acceptable severe accident provisions, and (4) achieving a design consistent with regulatory criteria. The key function of ALWR requirements here is to obtain meaningful agreements with the NRC, reflected in the SER, in these four areas.

5.2 Providing requirements for certification design

The second primary role of the ALWR requirements is to provide a set of standardized technical requirements to be met by suppliers in their certification designs. It is in the suppliers' interest to meet the ALWR requirements because of the stabilized regulatory basis established by the requirements and because the requirements reflect the needs and desires of the electric utility industry which has the nuclear plant operating experience and which is likely to be a key participant in any ALWR investment group.

5.3 Providing requirements for owner bid packages

The third primary role of the ALWR requirements is to serve as technical requirements for ALWR owner bid packages to design and license the standard plant. It is expected that any ALWR investor will insist on having an investment-ready design with high assurance of licensability. The ALWR requirements provide a foundation for this assurance, as shown on Figure III. Also, the ALWR requirements will be an input to the owner bid package to complete the detailed design and to construct.

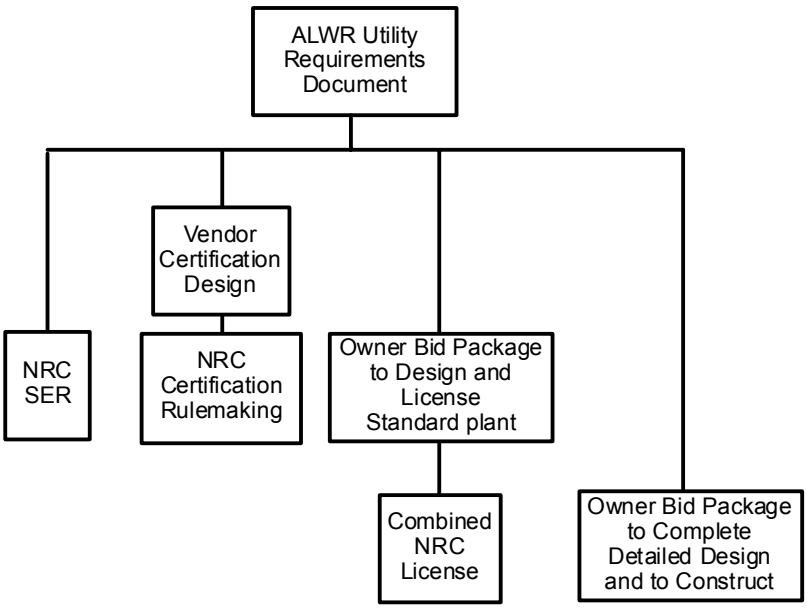


FIG. B1.3. Role of requirements in ALWR implementation.

6. CONCLUDING REMARKS

The URD is an important element within the process to develop new LWR designs for use in the twenty-first century. The policies and requirements embodied in the URD reflect the large volume of experience accumulated in operating LWR designs and therefore provide strong foundation for proceeding with confidence to develop and implement ALWRs that will meet the future needs of electrical energy suppliers.

The viability and utility of spending the time and resources to develop a set of utility requirements has been demonstrated in the early stages of the ALWR design process and will become increasingly evident as design are completed and plants are constructed and operated. As organizations in many countries around the world take the initiative to develop requirements specific to their needs, it has become clear that the requirements activity has become an essential step in the process for perspective owners and operators planning for the future implementation of nuclear power plants.

REFERENCES TO APPENDIX B1

[1] "Advanced Light Water Reactor Utility Requirements Document." Electric Power Research Institute, Palo Alto, California. Volume I, Rev 1, December 1995; Volume II & III, Rev 8, March 1999.

[2] "NRC Review of Electric Power Research Institute's Advanced Light Water Reactor Utility Requirements Document." NUREG-1242, Vol. 1&2, August 1992, Vol. 3, August 1994.

[3] "Strategic Plan for Building New Nuclear Power Plants." Nuclear Energy Institute Executive Committee, Washington D.C. Fifth Annual Update. November 1995.

APPENDIX B.2.

EUROPEAN UTILITY REQUIREMENTS
(provided by O. Andersson, FKA, Sweden)

1. GENERAL OBJECTIVES

Within Europe, the development, design and licensing of existing LWR plants have been performed on a national basis with little interaction between countries. To overcome this weakness, in late 1991 the major European electricity producers formed an organisation to develop the European Utility Requirements (EUR) document. Since that time the European Market (EU) has become reality and the vendors as well as the electricity producers are merging with their counterparts to form European groups.

The main objective of the EUR organisation is to produce a common set of utility requirements, endorsed by the major European electricity producers for the next generation of LWR nuclear power plants.

The requirements are addressed to the designers and suppliers of LWR plants. The aim of the requirements is to promote harmonisation of:

– The safety approaches, targets, criteria and assessment methods,
– the design conditions,
– design objectives and criteria for the main systems and equipment,
– equipment specifications and standards,
– information required for the assessment of safety, reliability and cost, and some of the corresponding criteria,

thus allowing the development of standard design that can be built and licensed in several European countries with only minor variations.

Although the requirements forms the basis for the procurement of new plants they may also have a wider application in the international market.

Benefits are expected in two fields:

1. Improvements in the licensing of new nuclear power plants and in their public acceptance:

- by setting common safety targets which are consistent with the best European and international objectives,
- by promoting within Europe common technical responses to safety problems,
- by setting "good neighbour" requirements, like low targets for accidents and routine radioactive releases to the environment, and consideration of decommissioning aspects at the design stage.

2. Strengthening of nuclear electricity competitiveness:

- by controlling construction cots and operating costs through standardisation, simplification and optimisation of maintenance at the design stage,
- by establishing stable conditions for competition between suppliers on the European Market,

- by allowing low operation and fuel cycle costs, through flexible and efficient design features that allow easy adaptation to future plant operating and fuel management schemes,
- by laying down ambitious (but achievable) availability and lifetime targets.

It is recognised that the full benefit of a common set of European utility requirements will be maximised if the requirements are in the mainstream of internationally accepted safety targets and developments in the nuclear design. Hence one of the main objectives of the EUR organisation is to ensure that the main EUR requirements are consistent with those developed for future nuclear plants by other utilities, regulators and international organisations. Moreover specific attention has been paid to the comments from those designers that develop new plants and from utilities that are a non-member of the EUR organisation.

In order to meet the economic targets of producing electricity from nuclear plants competitive costs, a high degree of standardisation is necessary, together with stability of the licensing regime. To facilitate this, the EUR document specifies site-related conditions that cover a wide range of European sites. Thus the EUR document sets out a framework in which a number of standard design could be developed and eventually built, and this in any of the participating European countries, with minimum adaptation to the basic design, and acceptable economic prospects.

2. EUR DOCUMENT STRUCTURE

The EUR document is structured into four volumes, each volume is divided into chapters that deal with a specific topic. The chapters are subdivided into sections.

- *Volume 1, Main policies and objectives:* this volume presents the major objectives of the EUR organisation and the main policies, which are implemented in the EUR document. It also summarises the most important requirements developed in volumes 2 and 4.

- *Volume 2, Generic nuclear island requirements:* this volume contains all the generic requirements and preferences of the EUR utilities for a nuclear island which are not related to any specific design.

- *Volume 3, Application of EUR to specific designs: this volume consists of a number of subsets.* Each subset is dedicated to a specific design that is of interest to the participating utilities. It contains a description of a standard nuclear island, a summary of the analysis of compliance versus the EUR volume 1 and 2, and, where needed, design dependent requirements and references of the EUR utilities. It also includes the information related to that design called for in certain requirements of volume 2.

- *Volume 4, Power generation plant requirements:* this volume contains the generic requirements related to the power generating plant. This volume is written as a complement to volume 2.

3. STRUCTURE OF VOLUME 2

The EUR policy is to have a core of strong generic requirements expressed as objectives or functions as far as possible. Several of these requirements are kept open, i.e. they provide only a design methodology and objectives that can be implemented in several ways by the plant designer.

Volume 2 contains chapters, which aim to tackle specific topics related to plant design and construction. Together they cover the whole scope of the activities that are necessary in order to design, license, build, test and operate at a nuclear island together with some of the related site facilities.

Volume 2 contains twenty chapters, as follows:

2.0 Introduction to the EUR volume 2
2.1 Safety requirements
2.2 Performance requirements
2.3 Grid requirements
2.4 Design basis
2.5 Codes and standards
2.6 Material related requirements
2.7 Functional requirements: components
2.8 Functional requirements: systems
2.9 Containment systems
2.10 Instrument & control and man-machine interface
2.11 Layout rules
2.12 Design process and documentation
2.13 Constructability
2.14 Operation, maintenance and procedures
2.15 Quality assurance
2.16 Decommissioning
2.17 PSA methodology
2.18 Performance assessment methodology
2.19 Cost assessment information requirements

Instrument & control and man-machine interface requirements

Introduction

EUR chapter 2.10 presents the general design and architecture criteria that are applicable to all instrument & control (I&C) and man-machine interface of an advanced LWR plant. The chapter addresses only I&C architecture and the related requirements. The specific functions to be performed by the I&C are not described in this chapter. These functional requirements can be found in chapters 2.8 and 2.9 and in each subset of volume 3 dedicated to a specific design.

Only digital I&C and computerised man-machine interface are considered in the chapter because this is considered to be the most credible option for plants to be designed and built within the next five or ten years.

All the requirements listed in the chapter are independent of existing solutions and I&C products. They are based upon technologies and experience available at the time the chapter is issued. They should provide an acceptable base for implementation of safety and licensing issues.

Scope and purpose of the chapter

In this chapter the requirements and rationales concerning I&C and man-machine interface (MMI) are described. General rules for the design of the I&C architecture are also given.

The main aspect to be considered as the basis for I&C design are identified and worked out. Emphasis is placed on the means to be developed with the aim of gaining appropriate definitions and analysis methodology to be considered in the I&C design, particularly in the fields of supervision and control of the power plant process.

Safety and economic aspects in the I&C and MMI system design and implementation have also been considered.

Organisation of the chapters

The order of the sections of the chapter attempts to follow the design process starting with the general principles and interactors, followed by analyses and design requirements and finishing with implementation. The aim is to simultaneously provide a list of requirements and a methodology that can fit all designs. It intends to give to the designer a frame of general principles that must be fulfilled and at the same time to allow him flexibility to optimise the solutions according to the design features and the state of the art at the time of the design activities. The MMI aspects are addressed together with the other topics and to not constitute a separate section.

The section headings are as follows:

- General principles for I&C design (2.10.2)
- Interactors and associated requirements (2.10.3)
- Functional analysis and assignments (2.10.4)
- Functional requirements for I&C design (2.10.5)
- Technical requirements for I&C design (2.10.6)
- Project implementation (2.10.7)

General principles for I&C design (2.10.2)

This section states the main objectives of I&C and establishes the links with the other chapters of the EUR.

Interactors and associated requirements (2.10.3)

The I&C system includes the major interface means of communication between the power plant process and the surrounding world.

Thus, when designing an I&C system, it is important to know the features and the needs of this surrounding world which involves various “Interactors”, human and non-human. This section defines the interactors and provides input for analyses and design.

Functional analysis and assignments (2.10.4)

Functional analysis has to be undertaken with the aim of designing I&C systems, which allows a high level of performance in the control of the power plant process.

This section deals with proven methodologies, which are to be used for this purpose. The main steps to be considered when performing analysis are:

- Identification of the goals to be attributed to a system,
- Development of a task analysis aiming to point out the means necessary to achieve these goals,
- Verification that the designed means allows the planned goals to performed effectively.

Functional requirements for I&C design (2.10.5)

This section addresses and develops the general directives of the EUR, which are applicable to I&C design and which are intended to reach the safety, availability and performance objectives. Some directives that are specifically related to I&C design are also added.

Briefly, the topics that is dealt with mainly concern:

- The safety classification of I&C functions and the categorisation of I&C equipment.
- The requirements associated with that classification and that categorisation,
- The safety policy, the rules and concepts which have basically to be used for I&C architecture design,
- The requirements and methodology that shall be used for the MMI design.

Technical requirements for I&C design (2.10.6)

This section is devoted to the development of experience practice, which has to be used for the specification and selection of equipment.

Topics that are addressed mainly concern technical aspects such as:

- Technology selection
- Standardisation
- Ergonomics and human factors for the MMI
- Instrumentation
- Electromagnetic compatibility
- Power supply
- Layout and cabling

Project implementation (2.10.7)

In this section, a review is made of the areas to be considered in each step of the I&C life cycle. It encompasses the miscellaneous aspects related to project management, I&C system security, Quality Assurance, design, specification, verification, installation, commissioning and operating phases.

Reference to applicable standards and their hierarchy can also be found in this section.

APPENDIX C

CLASSIFICATION OF SAFETY OR OPERATIONAL IMPORTANCE
(provided by H.M. HASHEMIAN)

IAEA Safety Guide 50-C-D establishes the concept of classification of nuclear power plant systems according to their importance to safety. It gives examples of the classification of the major systems of several types of nuclear power plants. Safety Guides 50-SG-D3 and 50-SG-D8 apply classification to I&C systems. These guides establish the distinction between the safety system and safety-related systems, which together form the systems important to safety. The safety system consists of the systems provided to ensure the safe shutdown of the reactor and heat removal from the core, and to limit the consequences of anticipated operational occurrences and accident conditions. Safety-related systems are systems important to safety which are not part of the safety system.

The principles of IAEA classification have been interpreted in IEC1226, which defines a method of safety categorization. The standard identifies categories A, B and C for functions, systems, and equipment of I&C systems that are important to safety. The definition of these categories are simplified as follows:

- Category A is assigned to functions, systems and equipment (FSE) which have a principal role in the achievement or maintenance of nuclear power plant safety.
- Category B is assigned to FSE which have a supporting safety role to systems of category A.
- Category C is assigned to FSE which have an auxiliary or indirect role in the achievement or maintenance of the nuclear power plant safety.

The remaining FSE are assigned to be “unclassified”, IEC1226 annex A gives examples of typical functions for each category. These examples are copied below from IEC1226:

Category A

Typical Functions

- reactor shutdown and maintenance of sub criticality
- decay heat transport to ultimate heat sink
- isolation of containment
- information for essential operator action

Typical Systems

- reactor protection system
- safety actuation system and safety system support features
- key instrumentation and displays to permit preplanned operator actions that are defined in the NPP operating instructions, and that are required to ensure NPP safety

Category B

Typical Functions

- 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 and controlling performance of individual systems and items of equipment during the post-accident phase to gain early warning of onset of problems, and to keep radioactive releases ALARA
- limiting the consequences of internal hazards
- monitoring / controlling handling of fuel where failure could cause a minor radioactive release

Typical Systems

- NPP automatic control system or preventative protection system
- control room data processing system
- fire suppression system
- safety circuits and interlocks of fuel handling systems used when the reactor is shut down

Category C

Typical Functions

- those necessary to warn of internal or external hazard (fire, flood, explosions, seismic events, etc.)
- those for which operating mistakes could cause minor radioactive releases, or lead to radioactive hazard to the NPP operating staff
- access control systems – communication systems to warn of significant on- or off-site releases for the purposes of implementing the NPP's emergency plan

Typical Systems

- alarm system
- radwaste stream monitoring and interlocks, area radiation monitoring
- access control system
- emergency communications

The categories of IEC1226 may be used in grading the I&C systems for identification of the relative importance of different influencing factors to different aspects of the requirements through the life cycle of an I&C system. Individual countries may have other methods of identification and categorization of FSE and items important to safety. These are defined through national and other standards.

The English language terms used in safety categorization are different in different nations, and the IAEA definition of "systems important to safety" includes two separate system classes, which are the "safety system" and the "safety-related systems". This differs from the terms used in US practice. The following chart illustrates differences between international

and different national practices. Decreasing importance to safety is indicated by movement to the right, and the vertical divisions are in qualitative terms.

Nuclear safety is not the only factor in determining the importance of an I&C system. It should be noted that IEC 1226 includes in category C some functions associated with more conventional concerns on personal and plant safety.

The utility may place a high requirement on a system than that required by safety considerations alone. This may be due to availability requirements, the importance of the system to plant operation, or due to the unique nature of the system design. The utility may then require a high level of assurance of performance and reliability. This can be given if the system is treated as if it belonged to a higher safety category, and is subject to more rigorous requirements than otherwise, for example, a utility may decide to require a high level of V&V for a computer-based system that is of critical importance to plant operation, although it has low importance to safety. This can be achieved if it is treated as if it belonged to a higher safety category.

Comparative Safety Classification and Safety Categories

<table>
<tr><td>National or International Standard</td><td colspan="5">Classification</td></tr>
<tr><td rowspan="2">IAEA</td><td colspan="3">Systems Important to Safety</td><td colspan="2" rowspan="2">Systems not important to safety</td></tr>
<tr><td>Safety system</td><td colspan="2">Safety related system</td></tr>
<tr><td>IEC 1226</td><td>Category A</td><td>Category B</td><td>Category C</td><td colspan="2">Unclassified</td></tr>
<tr><td>France N4</td><td>1E</td><td>2E</td><td colspan="3">IFC/NC</td></tr>
<tr><td>European Utilities Requirements (EUR) (time dependant)</td><td>F1A (Automatic)</td><td>F1B (Automatic and Manual)</td><td>F2</td><td colspan="2">Not Classified</td></tr>
<tr><td>UK</td><td colspan="2">Category 1</td><td>Category 2</td><td colspan="2">Not classified</td></tr>
<tr><td>USA (IEEE)</td><td>1E</td><td colspan="4">Non-nuclear safety</td></tr>
</table>

CONTRIBUTORS TO DRAFTING AND REVIEW

Anderson, O.	Forsmarks Kraftgrupp AB, Sweden	(2)
Bastl, W.	Institute for Safety Technology (ISTec) Ltd, Germany	(2)
Bock, H.W.	Framatome ANP GmbH, Germany	(1)
Han, J.B.	Korea Atomic Energy Research Institute, Republic of Korea, (2)	
Hashemian, H.M.	Analysis and Measurement Services Corporation, United States of America	(1,2)
Kang, K.S.	International Atomic Energy Agency	(1,2)
Karpeta, C.	SCIENTECH, Inc., Czech Republic	(1)
Kim, B.R.	Korea Institute of Nuclear Safety, Republic of Korea	(1)
Kotyza, V.	International Atomic Energy Agency	(1,2)
Lindner, A.	Institute for Safety Technology (ISTec) Ltd, Germany	(1)
Wahlström, B.	Technical Research Centre, Finland	(1,2)

Consultants Meetings

Vienna, Austria, 13–16 March 2001(1), 14–18 January 2002(2)