IAEA Nuclear Energy Series

No. NP-T-1.13

Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants

IAEA
International Atomic Energy Agency

IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A and VIII.C of its Statute, the IAEA is authorized to foster the exchange of scientific and technical information on the peaceful uses of atomic energy. The publications in the **IAEA Nuclear Energy Series** provide information in the areas of nuclear power, nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues that are relevant to all of the above mentioned areas. The structure of the IAEA Nuclear Energy Series comprises three levels: **1 — Basic Principles and Objectives**; **2 — Guides**; and **3 — Technical Reports**.

The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.

Nuclear Energy Series Objectives publications explain the expectations to be met in various areas at different stages of implementation.

Nuclear Energy Series Guides provide high level guidance on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.

Nuclear Energy Series Technical Reports provide additional, more detailed information on activities related to the various areas dealt with in the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series publications are coded as follows: **NG** — general; **NP** — nuclear power; **NF** — nuclear fuel; **NW** — radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA Internet site:

http://www.iaea.org/Publications/index.html

For further information, please contact the IAEA at PO Box 100, Vienna International Centre, 1400 Vienna, Austria.

All users of the IAEA Nuclear Energy Series publications are invited to inform the IAEA of experience in their use for the purpose of ensuring that they continue to meet user needs. Information may be provided via the IAEA Internet site, by post, at the address given above, or by email to Official.Mail@iaea.org.

TECHNICAL CHALLENGES IN THE APPLICATION AND LICENSING OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR ENERGY SERIES No. NP-T-1.13

TECHNICAL CHALLENGES IN THE APPLICATION AND LICENSING OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2015

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
November 2015
STI/PUB/1695

IAEA Library Cataloguing in Publication Data

Technical challenges in the application and licensing of digital instrumentation and control systems in nuclear power plants. — Vienna : International Atomic Energy Agency, 2015.
p. ; 30 cm. — (IAEA nuclear energy series, ISSN 1995–7807 ; no. NP-T-1.13)
STI/PUB/1695
ISBN 978–92–0–102915–7
Includes bibliographical references.

1. Nuclear power plants — Automatic control. 2. Nuclear power plants — Instruments. 3. Nuclear reactors — Control. 4. Digital control systems. I. International Atomic Energy Agency. II. Series.

IAEAL 15–00998

FOREWORD

One of the IAEA's statutory objectives is to "seek to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." One way this objective is achieved is through the publication of a range of technical series. Two of these are the IAEA Nuclear Energy Series and the IAEA Safety Standards Series.

According to Article III.A.6 of the IAEA Statute, the safety standards establish "standards of safety for protection of health and minimization of danger to life and property". The safety standards include the Safety Fundamentals, Safety Requirements and Safety Guides. These standards are written primarily in a regulatory style, and are binding on the IAEA for its own programmes. The principal users are the regulatory bodies in Member States and other national authorities.

The IAEA Nuclear Energy Series comprises reports designed to encourage and assist R&D on, and application of, nuclear energy for peaceful uses. This includes practical examples to be used by owners and operators of utilities in Member States, implementing organizations, academia, and government officials, among others. This information is presented in guides, reports on technology status and advances, and best practices for peaceful uses of nuclear energy based on inputs from international experts. The IAEA Nuclear Energy Series complements the IAEA Safety Standards Series.

The commercial nuclear power industry has started and is likely to continue to move forwards with digital instrumentation and control (I&C) upgrades and with new builds using digital I&C technology. The future of the industry will depend on solutions that comply with industry standards and that can provide a life cycle path for the long term operation of a plant. This movement is considered a fast transition from the proven analogue technology that the industry is currently based on.

This movement creates a significant number of technical, political, cultural and financial challenges. A considerable number of digital systems have been implemented in the existing global fleet, and also in new plants under construction, with digital platforms incorporated into the design.These system designs and implementations have brought a list of common challenges associated with them that continue to be confronted and debated by the industry today.

Numerous studies, workshops and forums have been organized by the IAEA, as well as by other organizations both national and international, to discuss the current digital I&C challenges faced in nuclear power plants, with one of the most important factors being how to approve, license and apply proposed designs. Different stakeholders currently have different understandings of the challenges, and of approaches to their resolution. These differences are significant enough to potentially affect the progress of the nuclear power industry. Setting the bar at unattainable levels will only hinder progress, and industry will ideally try to develop a common understanding and approach on how to apply and license new designs.

It should be pointed out that a single publication such as this one can only take the first step towards initiating a process leading to more consistent technical and licensing requirements. It is hoped that this publication will be used by the stakeholders that influence the requirements and will form a common sense approach to the digital I&C challenges currently being faced. This publication provides general and high level guidance in line with other industry reports and programmes to highlight the issues to operators, senior officials, regulators, vendors and all the support organizations engaged in the application and licensing of digital I&C systems.

A long term vision is needed for the nuclear community to move forwards in a consistent manner. Countries around the world are establishing new nuclear programmes and are relying on existing foundations to guide them to a safe and reliable future. The focus of all stakeholders should be on agreeing and driving forward the goal of commonality and harmonization, a goal to which this publication contributes.

This publication was produced by a committee of international experts and advisors from numerous countries, who are listed at the end of the publication. The IAEA wishes to thank all participants and their Member States for their valuable contributions, in particular, C. Scott (United States of America) for extensive assistance with the preparation of this publication. The IAEA officers responsible for this publication were O. Glöckler and J. Eiler of the Division of Nuclear Power and G. Johnson of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

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.

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

This publication has been prepared from the original material as submitted by the authors. The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this book and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

As the nuclear power industry modernizes existing analogue instrumentation and control (I&C) systems in current nuclear power plants to incorporate digital I&C technology, as well as implementing new digital I&C systems in new plants, the industry is faced with significant challenges. These challenges appear in the form of: uncertainty and inconsistency in developing and licensing digital I&C systems and equipment; difficulties in managing the necessarily incremental transition to more fully digital implementations; and technical complications arising from the enhanced functionality, highly integrated (and interdependent) architectures and flexible configurability enabled by digital technology. As 'soft' technology is inherent in digital systems, as opposed to the more strictly 'hard' technologies of traditional analogue systems, the benefits of expanded capabilities may be compromised by the burden of significant complexity. As a consequence, necessary functionality may be compromised by 'value added' functionality. Key characteristics, such as quality, reliability and deterministic behaviour, are difficult to confirm and almost impossible to quantify. In addition, system integrity is more complicated to maintain (e.g. enforcing configuration management and controlling the impact of human–system interaction).

1.2. OBJECTIVES

The goal of this publication is to present the technical challenges mentioned above to operators, developers, suppliers and regulators so that the industry can capture and benefit from shared experience, recent technology developments and emerging best practices. The publication discusses the technical challenges of designing, developing, implementing, licensing and maintaining digital I&C systems, rather than examining the various vendor specific product lines, plant specific architectures and country specific licensing frameworks and processes. The final objective is to help industry stakeholders move towards effective resolution and a more common position on these technical issues, thereby providing the industry with the confidence to move forwards with improved designs for existing and for new plants. Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

1.3. SCOPE

This publication highlights the technical challenges, significant issues and credible available options, along with associated existing precedents, for resolving these problems. The related benefits and challenges of each option are also discussed. However, it is not within the scope of this work to give comprehensive technical solutions to these issues or to develop a unified regulatory framework for consistent licensing.

It is intended that this publication will be used by regulators, operators, vendor organizations and other stakeholders to develop a better understanding of the need for consistent approaches in the application of digital I&C. The industry is encouraged to engage in discussions on the issues presented in this publication to create harmonization and a positive path forward to allow for a consistent, safe and cost effective model to implement digital I&C systems in the future.

1.4. STRUCTURE

This publication contains four main sections. Section 1 introduces the topic and the objectives of this publication. Section 2 discusses the common features and challenges in current methodologies of implementing and licensing digital I&C systems. Section 3 describes 17 important issues in detail. Each of the 17 issues is divided into the following categories:

- Introduction: This describes the issue of concern, with some background and the associated challenges.
- Options: This describes different options that can be taken to mitigate or resolve the issue at hand.
- Associated benefits and challenges: This outlines the benefits and challenges posed by each of the suggested options.
- Precedent decisions / country experience: This highlights some of the precedents that have been implemented in the nuclear industry related to the issue of concern.
- Recommendations: This section describes suggested recommendations based on the experience of nuclear industry experts from operators, regulators, vendors, agencies and research organizations. These recommendations form guidance on good practices and are not recommendations based on Member State consensus.

The 17 issues (not in order of priority/importance) discussed in detail in Section 3 are:

- Self-diagnostics within a digital I&C platform;
- Independent verification and validation (IV&V);
- Management of the functional requirements specification;
- Development of and adherence to configuration management;
- Common cause failure (CCF), diversity and defence in depth;
- Use of smart devices;
- Safety classification schemes;
- Computer security;
- Harmonization of standards;
- Taking credit for on-line monitoring;
- Environmental qualification of safety system platforms;
- Impact of hardware description language (HDL) programmable devices;
- Digital communications;
- Safety classification and function of a soft controller;
- Formal methods of software development;
- Use of wireless technology;
- Reliability (taking credit for digital systems in probabilistic risk assessment (PRA)).

Section 4 provides a summary of this publication.

The International Electrotechnical Committee (IEC), the Institute of Electrical and Electronics Engineers (IEEE), other standards bodies, regulatory bodies, industry, research and development (R&D) and technical support organizations, universities and several other national and international organizations have also developed their own technical documents and guidance for the application of I&C. An extensive list of these important guides, codes and standards is provided in the IAEA Nuclear Energy Series publication entitled Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants [1].

The Glossary provides definitions of terminology in use within the nuclear I&C area, based mainly on the IAEA Safety Glossary [2] and other internationally recognized publications. A list of abbreviations that are used throughout the main text is given at the end of this publication.

2. THE CHALLENGES OF CURRENT LICENSING PRACTICES

2.1. CURRENT FEATURES OF DIGITAL INSTRUMENTATION AND CONTROL LICENSING

When considering local conditions, current licensing processes normally follow practices that reflect national legislation. National requirements typically have a history that is based on an industrial tradition and the way that nuclear power was introduced. Thus, a variety of national requirements have been created, sometimes perhaps even with the intention of protecting specific national interests. Coordination of these various national approaches is not yet common practice. This causes many drawbacks for the entire nuclear industry, including developers, vendors, operators and even the regulators themselves.

National regulators are interested in and familiarize themselves with regulations that are being applied in the nuclear industry in other countries. However, experience shows that there are challenges in appreciating how requirements are applied in other countries with nuclear power programmes. Deviations in national regulations may include:

— A lack of precedent in developing common technical responses to safety issues;
— A lack of established requirements that are considered valid across many countries that are involved in the nuclear energy industry.

From the viewpoint of the general public, national regulations may not always be transparent and easy to understand. A set of general principles, including agreed terminology and phrasing, which is readily understandable by all interested stakeholders, is not available worldwide.

There is clearly a need for better international coordination of the licensing requirements of digital I&C. Without coordination and consistency, it is difficult to find cost effective approaches to the licensing of digital I&C around the world, which could lead to the introduction of unnecessarily complex solutions.

In spite of the increasing globalization of nuclear utilities and of I&C vendors, there are safety system architectures that are considered acceptable in some countries but which are not accepted in others. Although this may be connected to the specifics of the nuclear site itself or its environment, in many cases, the reason does not arise from this fact, but from the differing regulations (including guidelines and review approaches) of different countries.

Variations in systems of requirements in different countries are not always understood. In many technical areas, a comparison of important documents to see where they agree and where they differ is still missing. Another issue, which may warrant in-depth discussions, is the structure of requirement systems. A good description of relationships between different requirements systems and between different hierarchical requirement levels is currently lacking. The diversified situation may put a burden on national regulators, because it is a large effort to maintain national requirements that are up to date.

The diversified situation of multiple regulatory regimes causes uncertainties in the estimates of time and resources to be used in the licensing process. For vendors, this situation makes it more difficult to reuse their technical solutions for a large spectrum of applications and makes this industry a challenging market to serve. It also makes it commercially less attractive for companies to create specialized tools for design and verification of software to be used for digital I&C applications in nuclear power plants.

A lack of coordination leads to poor understanding of the roles, tasks and actions of operators, vendors and authorities in I&C design and implementation projects. This results in increased costs and reduced predictability in project execution. The diversified licensing requirements also make the licensing process less transparent and understandable, especially for non-experts in I&C technology.

Currently, national regulators often apply both national and international codes and standards. However, the influence of international codes and standards is often relatively weak when compared with that of national requirements. This poor reliance on international standards in the licensing process makes the results of a specific licensing activity more challenging to use for other plants and in different countries.

Various R&D projects in different countries have been carried out to establish a basis for licensing digital I&C, which has led to a situation where a large variety of national approaches have been developed.

Limited advances towards greater commonality with other industries that use I&C to manage significant hazards have been made so far. This inhibits the market from being more competitive in the nuclear area, limits the experience base and discourages investment in improved functionality and quality available for the nuclear I&C industry. (One achievement is IEC 61508 [3], which is implemented by IEC 61513 [4] for the nuclear industry, and also IEC 61511 [5] for the chemical, oil and gas processing industries.)

As there is a large diversity in national requirements for digital I&C, it is not likely that harmonization will be achieved in the short term. To initiate and promote harmonization, the IAEA has prepared general and high level guidance to assist the licensing of digital I&C, and published IAEA-TECDOC-1327, Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants [6], in 2002. However, no significant steps have been taken since to reach a higher level of international harmonization.

2.2. DISADVANTAGES OF CURRENT PRACTICES

The lack of a common safety philosophy is the most important obstacle for harmonization. One evident example of this is the large number of differing safety classification systems in IAEA Member States. Practice has shown that it is sometimes difficult, if not impossible, to agree upon a common classification approach, which is important for easing discussions and achieving harmonization.

In a situation where there is no agreement on comprehensive guidance documents, there is also the danger that a combination of requirements from different sets of standards may introduce difficulties with consistent interpretation. The problem is thus not the absence of guidance, but rather in determining what guidance to use and how it should be used.

To some extent, national licensing authorities have been incorporating available standards into their requirements, but they have also produced their own requirements and guidelines. This development has reflected issues and challenges in the application of new technology, but it has also incorporated 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 new technology difficult for the parties involved in the licensing process. For example, one issue to resolve has been how specific solutions that have been created within one system of standards could be evaluated in another system. In their refurbishment projects, nuclear operators have sometimes found it difficult to establish and argue for a specific set of requirements to be used. Experience has shown that vendors can have difficulties trying to interpret and address the variations among national requirements and different sets of comparable standards. Finally, there have also been cases where national licensing authorities have found it challenging to manage the assessment of a variety of technical solutions based on different guidelines and national/organizational conventions in the context of their own regulatory regime.

The lack of harmonization compromises the efficiency of national regulatory processes as follows:

— The effectiveness and efficiency of regulatory design reviews are decreased owing to the extreme difficulty that vendors have in producing a fully standardized design.
— Mutual sharing of experience is limited owing to the lack of harmonized requirements in design and manufacturing.
— Knowledge transfer regarding regulatory issues and practices is also limited owing to the lack of harmonized requirements.
— International cooperation among regulators is limited in some areas, which leads to poor understanding of different regulatory positions and prevents agreement on the most convincing and reasonable solutions.
— Uncertainties exist in the licensing processes, which currently discourage the adoption of new systems and technology.
— Difficulties emerge with the reuse of previously licensed technical solutions for a large spectrum of applications and hence make them less commercially viable.
— Higher complexity and risks emerge in licensing I&C systems for modernization projects and new installations, without any discernible safety benefits, and, at the same time, resulting in higher costs and increased effort.
— Limitations exist in the development of competency on a global basis, thus making the resolution of complex licensing issues more difficult.

3. IMPORTANT ISSUES FOR CONSIDERATION

The following section identifies what are considered to be some of the most important issues encountered in digital I&C system design, licensing and implementation. These issues are not addressed or identified for the first time in this publication, but have been the subject of many discussions, forums and meetings among regulators, operators, vendors and others engaged in digital I&C design. The purpose of the identification of these issues is for all of the users of this publication to be aware of the potential issue of challenge and also be aware of what options are in place to address the issue, in addition to moving towards a more coordinated position to reduce the challenges associated with each issue.

This publication identifies 17 important issues (not in order of priority or importance) related to digital I&C systems, and also assesses the more common challenges faced with the issues identified. The lists of challenges should not be considered to be comprehensive, as further challenges may be encountered as understanding of the issues develops.

3.1. ISSUE No. 1: SELF-DIAGNOSTICS WITHIN A DIGITAL INSTRUMENTATION AND CONTROL PLATFORM

3.1.1. Introduction

One of the potential benefits of digital I&C platforms is the capability for extensive diagnostics. This is a benefit not available in analogue systems, and yet is a challenge from a licensing perspective. Many digital platforms have embedded diagnostics that are executed continuously within the operating cycles of the platform. These diagnostics can test many different system and application parameters. For example, diagnostics can be used to check internal calibration and determine the health status. A significant proportion of these diagnostic functions can also contribute to the assurance of the safety integrity of the platform itself.

Fail-safe design of computer based systems important to safety will inevitably use on-board self-diagnostics to ensure that failures are detected, and as a result, will use appropriate default states attained by the system. In this way, the failures will be revealed, which will allow the repair and replacement of the failed component (computer board), hence maximizing the system availability. These on-board self-diagnostics are usually designed to check the integrity of the memory, input/output capabilities, processor functionality, etc. The diagnostic processes are usually split between initialization (prior to the initiation of the control or protection application) and diagnostics, which run in parallel with the application code.

Ideally, self-diagnostics would provide comprehensive coverage of the failure mechanisms within the computer boards. However, this is not always possible, and it can be difficult to conclusively prove that the diagnostics can provide 100% coverage of all board faults.

Hence, it is necessary to make a conservative assumption about the percentage of board failures that the self-diagnostics will identify. This is usually a judgement based on the extent of the self-diagnostics and the complexity of the computer boards, and is often supported by a component level failure modes and effects analysis. Benchmarking against other previously assessed computer boards is useful in supporting this judgement.

By combining the percentage of failures that are detected by the self-diagnostics with the predicted board failure rate, the unrevealed failure rate can be calculated.

As there are potential unrevealed failures, some of which may be unsafe failures, there is still a need to perform functional testing of the system in order to ensure that there are no unsafe failures remaining in the system. The use of self-diagnostics will help to reduce the extent of the functional testing, but will not eliminate the need for this testing.

The main purpose of diagnostics is to increase reliability, so introducing self-diagnostics has benefits, even if the volume of surveillance tests cannot be reduced. With periodic testing, some faults may remain undetected until the next periodic test, or in the worst case, until functional failure. The probability of these events can be greatly reduced using self-diagnostics.

In the United Kingdom, on-board self-diagnostics are used within computer based protection systems for the advanced gas cooled reactor fuel routes and the primary protection system (PPS) for Sizewell B nuclear power plant. The initial assumption for the percentage of failures revealed by the self-diagnostics was that 90% has been considered a conservative figure. However, in the case of the PPS for Sizewell B, the percentage coverage was increased for certain boards based on the ability of the self-diagnostics to detect faults. In order to justify the higher figure, the arguments had to be clearly stated in the reliability assessment for the system.

In addition to the use of self-diagnostics, the PPS undergoes a full functional test on all redundant divisions once a month. By combining the effectiveness of the self-diagnostics, the failure rates of the individual boards and the monthly functional test, a target reliability figure of 10^{-4} probability of failure on demand has been claimed for the system.

Many regulators are reluctant to accept the use of self-diagnostics to replace surveillance testing because there are limited standards and guidelines and also because of the difficulty in proving the level of coverage. There have been a number of regulators who have allowed credit for diagnostics to reduce the scope and/or frequency of surveillances.

3.1.2. Options

— Use the inherent capabilities of the computer based I&C systems to provide self-diagnostics and take credit for this when specifying the system surveillance requirements.
— Take no credit for the self-diagnostics, and instead employ additional equipment and procedures specifically to satisfy requirements for the safety system surveillance tests.

3.1.3. Associated benefits and challenges

3.1.3.1. Benefits

The benefits of these types of diagnostics are that there could be a case developed to allow the licensee to reduce the amount of manual testing. For example, a platform could perform diagnostics such that the reduction of the monthly surveillance testing might be justified. The benefits from reducing surveillances are potentially significant. When operating a plant, any reduction in the amount of manual intervention required with control equipment for testing has a benefit through the reduction in risk of a trip. An unnecessary trip stresses the plant safety systems and, in the longer term, can affect the safety limits of the plant. In addition, the trip entails a significant financial loss. The reduction in manual testing also frees staff to attend to their primary safety roles as well as saving maintenance costs.

3.1.3.2. Challenges

There are no comprehensive guidelines in the nuclear sector such as standards for surveillance tests using self-diagnostics features.

However, the IEC 60671 standard [7] published in 2007 identifies computer self-supervision as an alternative to periodic surveillance testing by self-diagnostics. For the industry to benefit from digital systems, the advantages of these systems need to be used. Regulators may be conservatively positioned on this issue because few precedents have been set and a full understanding of and confidence in the digital capabilities of the computer based systems are not yet fully realized.

In addition, there is a trade-off between the benefits provided by self-diagnostics and the increased complexity that they bring to the system. For example, IEEE 7-4.3.2-2003 [8] states that “Safety systems should be as simple as possible; therefore, functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system”. Similarly, in the UK, the regulator [9] recognizes that:

> “There can be undesirable effects in that the level of complexity is increased. The aim should always be that the elements carrying out the diagnostic function, and the diagnostic function itself, should not be able to interfere adversely with the safety function. Provided this criterion is met then the presence of self-testing is beneficial. However if it is not met, for example in systems with embedded software where the processor

that implements the safety function also implements the self-tests, then there is a significant danger that the self-test functions can interfere with the safety function. In such cases it is not appropriate to assume that the benefit to safety of self-testing outweighs the dis-benefit to safety of increased complexity, and if such a device is to be used then its safety analysis needs to encompass the self-testing software."

3.1.4. Precedent decisions / country experience

Testing surveillances for digital I&C systems have been reduced at some plants, such as the N4 plants in France, and the Tianwan and LingAo 2 nuclear power plants in China.

3.1.4.1. Experience in the United States of America

In the safety evaluation report (SER) on the licence amendment request to upgrade the safety systems at the Oconee nuclear power plant [10], the United States Nuclear Regulatory Commission (NRC) authorized surveillance extension of the channel functional test (CFT) based on the credit provided to the self-diagnostics in the approved platform. The regulatory position is expressed in the following SER text [10]:

"Revision of the current TS [technical specification] SR [surveillance requirement] is the performance of CFT on a 92-day 'Frequency for Unit(s)' with the ESPS digital upgrade not complete and an 18-month Frequency for Unit(s) with the ESPS digital upgrade complete. The licensee stated in the TS bases that for Unit(s) with the ESPS digital upgrade not complete, the 92-day frequency is based on operating experience that demonstrates the rarity of more than one channel failing within the same interval. Also for unit(s) with the ESPS digital upgrade complete, the 18-month frequency is based on the design capabilities and reliability of the new digital ESPS. The digital ESPS software performs a continuous online automated cross channel check, separately for each channel, and continuous online signal error detection and validation. The protection system also performs continual online hardware monitoring. The 18-month CFT validates the self-monitoring function and checks for a small set of failure modes that are undetectable by the self-monitoring function for unit(s) with the ESPS digital upgrade complete, the digital processors shall be rebooted as part of the functional test. This verifies that the software and setpoints have not changed. Additionally, the reliability of components whose failure modes are not automatically detected or indicated but also support a test frequency of 18 months."

3.1.5. Recommendations

— Applicants should take credit for self-diagnostics to reduce surveillance requirements.
— Standards will ideally be updated to give guidance on the use of self-diagnostics as part of surveillance testing activities.

3.2. ISSUE No. 2: INDEPENDENT VERIFICATION AND VALIDATION

3.2.1. Introduction

3.2.1.1. Independent verification

The verification process covers both the review of the software against its supporting documentation (software requirements specification and software design) and verification as required. Tools used for the verification should be controlled as part of the overall configuration control of software, documentation, development and verification tools.

Verification is only complete when all of the anomalies and findings have been addressed to the satisfaction of the verification team.

At that point, the software is declared to be verified and the software version changed within the configuration management system to reflect this. The software can then be used in a subsequent stage of the development process such as integration and functional testing.

3.2.1.2. Peer review

The peer review is a desktop review of the code or code changes performed by a member of the development team who is not the author of the code or change. The review will confirm either that the code matches its specification or that the code changes match the design change definition and that the work done adheres to the appropriate coding standards. The peer review follows an agreed peer review plan that covers the scope and depth of the review (as part of the overall system quality plan).

3.2.1.3. Validation

Validation is taken to be the testing activities post-verification. The testing includes functional testing of the integrated software. Quite often, this will include testing on test beds (off-line testing) and the complete system (on-line testing).

As part of software development, an important element of verification and validation (V&V) is independent review. When a platform is submitted for assessment, the operating system being used must be developed under strict guidance and also must have demonstrated that it has undergone a rigorous IV&V programme. Inclusive of this, the application software development should also undergo this same level of effort in order to be acceptable for use in a safety system.

There are several standards and technical reports that give guidance on how IV&V should be performed. Examples include the IEEE Standard 1012 [11] and various IAEA publications [12–14]. A significant issue related in this guidance is the definition of independence. Some guidance describes independence as follows: the IV&V organization should be one that is completely independent from the developing organization from any technical, management and financial ties. This may be interpreted differently in Member States.

The European Union regulators common position report [15] defines IV&V as follows:

> "Proposed software changes shall be analysed and reviewed for effect on safety, by suitably qualified and experienced staff — e.g. manufacturers (suppliers), system designers, safety analysts, plant and operational staff — that are independent from those persons proposing, designing and implementing the change. The analysis and review shall consider manufacturers (suppliers) V&V and independent assessment reports, as well as test specifications and test reports, or other such documentation as appropriate to the change being proposed. The results of the analysis and review shall be documented and shall include a recommendation for approval, or rejection of the change from the safety perspective."

For systems performing Category A functions, there is a mandatory requirement for IV&V of the software and the software documentation. Two key requirements apply to the teams performing these activities:

— They must be independent from designers.
— They must have different management reporting lines.

For systems performing lower category functions, formal independent verification is not a mandatory requirement. However, a less rigorous peer review is required for such systems.

The requirements for independent verification (or peer review) and validation apply to both initial system development and subsequent modifications to the software. The need to carry out these activities for modifications ensures that the safety remains valid and hence the requirement to carry out verification (peer review) and validation on modifications to the software is captured within the modification process and procedures.

3.2.2. Options

The key issue is whether the designing body is required to seek a third party to complete the IV&V or to provide internal independence within the company to perform IV&V:

— Some regulators deem it acceptable to have an independent group within the same company perform the IV&V as long as technical and management independence is in place.
— Other regulators insist that a third party company perform the IV&V to ensure absolute independence, even at the financial level.
— A third option is to allow the end user to perform the IV&V.

3.2.3. Associated benefits and challenges

3.2.3.1. Benefits for the first option

An essential characteristic when performing IV&V is to have the necessary knowledge to understand the requirements for the platform, system and application. Product knowledge is generally available to support internal IV&V, thereby reducing the cost and also minimizing the technology exposure to outside sources. This also reduces training and schedule risks.

3.2.3.2. Challenges for the first option

If the IV&V is performed internally, it can be argued that the management pressure to meet the schedule and costs could compromise the quality of the IV&V.

3.2.3.3. Benefits for the second option

Complete independence is achieved from a management, technical and financial aspect. This provides assurance that internal influences will not compromise the IV&V task.

3.2.3.4. Challenges for the second option

It is more difficult to manage a third party company; therefore, cost and schedule risks are potentially high. Having a third party perform the IV&V requires training on the platform and also may lead to release of potentially proprietary information.

3.2.3.5. Benefits for the third option

If the end user performs the IV&V, they ultimately control the schedule and also become familiar with the platform to be installed in their facility. This encourages the development of intelligent customers, which can have significant lifetime benefits in system management.

3.2.3.6. Challenges for the third option

In many cases, the end user does not have the domain knowledge or the appropriate staffing to support these efforts.

3.2.4. Precedent decisions / country experience

The NRC, the Korea Institute of Nuclear Safety (KINS), the Canadian Nuclear Safety Commission and the Ukrainian State Nuclear Regulatory Committee have accepted the first option.

For safety I&C system modernization in Hungary, the development was performed by the vendor using an engineering tool. The IV&V was performed by an independent organization and the nuclear power plant end user.

The nuclear power plant staff developed the system on a simulator using a formal specification tool, fully independently from the vendor. The inputs for this development came from the same high level logic diagrams used by the vendor for their system.

The verification process was performed by comparing the developed system with the specifications at every level. The validation comprised the final comparison of the two separately developed systems (simulator representation and the real reactor protection system (RPS)) using the full scope simulator. For this purpose, the simulator architecture was modified to provide the comparison capability. For any further I&C system validation (modernization or I&C system for a new plant), the same approach can be applied.

Although several verification steps (verification loops) in a system development process may be executed correctly, it is difficult for the final validation of a complex system to cover all details of the system. This difficulty comes mainly from the fact that it is not possible to generate all the events (e.g. postulated initiating events (PIEs)) against which a protection system has been designed.

3.2.5. Recommendation

IV&V performed in accordance with the accepted international standards of the first option is acceptable.

3.3. ISSUE No. 3: MANAGEMENT OF THE FUNCTIONAL REQUIREMENTS SPECIFICATION

3.3.1. Introduction

Well managed I&C requirements establish the technical basis for an I&C system design or project. The definition of correct, consistent, unambiguous and identifiable requirements, both functional and non-functional, enables straightforward specification design, a relatively simple V&V process and the necessary analysis and assessments to be undertaken. Defining requirements starts from the requirements for I&C system architecture, after which the system requirements specifications can be elaborated. The system specification is the basis for subsystem or software requirements.

This area is a major concern for the successful outcome of digital I&C projects, and can also potentially affect the reliability, safety and licensing of the systems. IAEA-TECDOC-1066 [16] identified that plants that have introduced upgrades of analogue systems using digital equipment have encountered a large variability in costs and problems, and that the source of many of the problems could be traced to the specifications for the upgrades. Similarly, a UK Health and Safety Executive survey [17] of control system incidents that had been reported to them found that a significant percentage of the incidents could be attributed to inadequacies in the specification of the control system. Problems can arise because of insufficient understanding of the functions to be performed by the systems, as this knowledge lies at the interface between the plant process and I&C system disciplines. There is often also a knowledge management problem for existing plants in that the original knowledge is not readily available, the plant design principles and documentation may be dispersed, and there may not be a high degree of assurance that the facility documentation reflects actual plant status after years of cumulative modifications [1].

It is important for developers to be involved in requirements management (RM), as the purpose of RM is to establish a common understanding between the customer and vendors. That common understanding is the basis for planning and managing the project. Developers can play a crucial role and should be involved early on with the requirements specification, and continue to help clarify and refine requirements as these evolve through the iterative development life cycle. Developers are responsible for turning concepts into reality, so the sooner they take an active role in the requirements process, the greater the likelihood that the requirements can be accurately translated into a workable system within the defined time schedule. However, this early involvement is often not possible, as requirements are normally fixed before suppliers are selected.

Studies such as the Standish Group report entitled Chaos [18] have shown that requirement errors are the most difficult and expensive errors to fix (and the longer they go uncorrected, the more costly they become). Starting with a requirement that is ambiguous, or changes in the middle of the development life cycle, can invalidate the design and result in expensive architectural rework, ineffective validation tests, incorrect documentation, and so on. More time will be spent fixing problems that could often have been avoided in the first place.

Good RM practices may not be explicitly enforced under all regulatory regimes, or the level of rigour required may differ. In general, the more informal the RM process is, the greater the risk is that the solution will not fulfil the safety requirements. Common arguments for adopting a less formal RM process may be that it allows faster development, provides more flexibility or that formal requirements documents are not needed. Unfortunately, these decisions often have far reaching negative consequences. Consequently, a development team needs to determine the degree of RM formalism required for the success of the project. Fundamentally, RM practices should yield requirements that are clearly understood by all team members, exert control over changing requirements and enable effective communication to keep the entire project team focused on a consistent objective.

In certain cases, adhering to a very formal RM practice might seem too onerous, for example, following a traditional change control process that includes obtaining approvals from a change control board might act as a bottleneck to software delivery. However, even in this instance, the team would benefit from using selective RM techniques, such as storyboards or prototypes, to validate ideas before committing to developing and delivering them. At the other extreme are cases that demand strict adherence to formal RM practices. For example, developing software for an RPS will require a highly structured RM process, because making a mistake with a requirement in this situation could lead to significant consequences.

'Good' system requirements are:

— Attainable;
— Testable;
— Verifiable;
— Traceable.

The first three features basically provide for a workable and concise requirements document that is easy to develop and maintain. The traceability feature of the requirements specification may significantly save time during design reviews, where understanding of the basis for a requirement may be the most time consuming activity.

There are a number of standards and guidelines that might be used to develop requirements. For system requirements specification, many vendors in the nuclear industry use IEEE Standard 1233 [19], and for software requirements specifications, IEEE Standard 830 [20] may be considered an adequate starting point.

3.3.1.1. Automating requirements management

Many vendors are improving the methods they use to gather, analyse, document and manage their requirements. Project teams traditionally document their requirements in a structured system or software requirements specification written in natural language. However, a document based system requirements specification (SyRS) has some limitations because it is difficult to keep up to date, difficult to communicate changes to the affected team members and difficult to define links between functional requirements and corresponding use cases, designs, codes, tests and project tasks.

A commercial RM tool that stores requirements and related information in a multiuser database provides a more robust solution. These tools provide functions to manipulate and view the database contents, import and export requirements, define links between requirements and connect requirements to other software development tools.

Many plant vendors already use automated tools for RM. Each organization should define which of these tools fits best into internally accepted design processes. Controlling requirements for a complex project is a tedious technical task that is very difficult to manage without effective software tools, which can help with many tasks. Traceability is very important. Tracing individual requirements to system components helps to ensure that no requirements are omitted during implementation, and allows links to be established between different kinds of requirements also between other objects such as codes, test cases, analyses, and so on. Most significantly, when analysing the impact of a change proposed in a specific requirement, the traceability links reveal the other system elements that the change might affect.

3.3.1.2. Concerns

— The lesson learned from different projects is that about 80% of project cost overrun is related to poorly developed requirements. This kind of problem significantly increases the time spent on design reviews and the project baseline changes due to requirements creep, and generally due to the whole project life cycle activities.
— Before the project contract is signed, the contract may be satisfactory for the main requirements at a preliminary level, that is, the preliminary safety analysis report may be adequate. However, after the project starts, the design work may begin directly at the system specification level. In this case, the architectural requirements and specification do not develop from the state that prevailed before the project started and the detailed design could conflict with the original design basis.
— In some cases, the requirements are too general. There should be unambiguous technical and project related statements. Direct citations from design basis documents, such as standards or regulatory guides, should be avoided unless there are clear technical requirements.
— It is valuable to employ a suitable tool to follow the requirements through the various design phases. This can ease the V&V activities and safety assessments.
— The approach to licensing digital systems important to safety should be clearly understood and accepted by the development team at an early stage in the project, as licensing issues (e.g. requirements for mitigation of CCF vulnerability) have the potential to cause very significant changes to the I&C system requirements, architecture and design.

3.3.2. Options

International standards provide a solid basis for RM. IEC 61513 [4] provides a model for a requirements hierarchy, starting at the architectural level. IEEE standards such as IEEE 1012 [11] describe a model of phased design process, which provides a basis for sound RM. IEEE 1233 [19] and IEEE 830 [20] provide suitable starting points in developing system and software requirements, respectively. IAEA-TECDOC-1066 [16] provides guidance to help establish, at each life cycle phase, the relevant stakeholders, objectives, inputs, constraints, outputs, and so on.

It is valuable to include the RM plan in the project quality plan, which is typically reviewed by regulators. The RM plan presents the methods, responsibilities and tools used in the RM process. This plan may often be defined in the system quality plan.

RM is purely a management and technical process. The differences in the national practices can be in:

— How early, if at all, the requirements are reviewed with the customer and any third party.
— How detailed the management process is required to be.

3.3.3. Associated benefits and challenges

3.3.3.1. Benefits

IAEA-TECDOC-1066 [16] identifies that:

> “The provision of complete and clear specification documents and plans will encourage good communication and will reduce the chance of misunderstandings between utility, design authority and supplier. It applies to the personnel involved in manufacture, software design and production, and testing and installation processes. It will finally contribute to a successful achievement of the upgrading goal, whether this is relevant to plant safety or operability.”

While the context of the TECDOC is digital upgrades, these benefits apply equally to new build projects.

3.3.3.2. Challenges

As discussed in IAEA-TECDOC-1066 [16]:

"At present, there is no methodology, standard or guidelines generally accepted by the nuclear industry for preparing the various types of requirement specifications and plans for digital upgrades. This can be contrasted with the design and implementation…of computer software after the requirements have been defined. For software, there are many detailed and specific standards on the methodology and the detailed contents of the different specifications and design documents used in the lifecycle. For refits and upgrades, frequently the specifications of requirements for an analog system are reused and slightly modified to define the upgrade. This has often resulted in difficulties. In some cases, the documentation of the existing power plant may be inadequate for the complete definition of the requirements. Additional work may be required to determine features needed for the new equipment. Usually, digital equipment is needed with functionality different to or greater than the original systems. The specifications of requirements, manufacture and test must therefore include important requirements beyond the scope of the original analog equipment. Preparation of good specifications for a digital upgrade requires expertise in hardware, software, data communications, plant operations, networking and licensing."

From this, the major challenges can be summarized thus:

— There is little guidance available for preparing system level requirements.
— Digital I&C systems generally have functionalities that are different to traditional analogue I&C systems.
— Definition of system level requirements requires expertise from many different domains and often falls across organizational boundaries with multiple important stakeholders involved.

3.3.4. Precedent decisions / country experience

During a safety I&C system modernization in Hungary, the following specification approach was used:

Specification of process requirements → Natural language description of tasks → Specifications in a formal language (high level and then detailed logic diagrams) → Testing and return to previous stages if necessary → Engineering → Testing and return to previous stages if necessary → Implementation → Validation and return to previous stages if necessary → Final installation. This could be a good model for a safety system development process.

The Ukrainian State Nuclear Regulatory Committee requires that the implementation of RM and SyRS safety reviews be part of the licensing process. A typical SyRS for Ukrainian safety I&C modernization includes safety requirements elements and functional requirements elements, including application logic diagrams. All requirement changes are implemented under change control procedures at any stage of the system life cycle. The question of using an electronic format of SyRS has not yet been considered by the Ukrainian regulator.

3.3.5. Recommendations

— Initial feasibility studies can be very useful to establish customer expectations, the safety role of the equipment and the extent of use of digital systems.
— A clear scope and division of work should be defined because of the different knowledge domains involved.
— The safety authority approach to licensing digital systems that are important to safety should be clearly appreciated and agreed by the project at an early stage in the project.
— The use of requirements automation tools to improve the design process and minimize errors in the RM process should be considered.
— A clear and reasonably stable I&C design basis should be established early in the I&C system development process.

3.4. ISSUE No. 4: DEVELOPMENT OF AND ADHERENCE TO CONFIGURATION MANAGEMENT

3.4.1. Introduction

Configuration management provides a means to control the design, test and installation status of an I&C project. Configuration management goes from the I&C system architecture specification level to the software and hardware configuration level. The I&C architecture configuration should be consistent with the configuration of the plant process systems ('design freezes'). Configuration management is essential for well controlled design changes:

— The configuration should be well managed at the system software and hardware level. Configuration management should also address tools and other support software. This contributes to successful modification of software and hardware.
— Higher level documents, such as system specifications and requirements, should be covered by configuration management. Proper management of a well defined system configuration ensures consistency throughout the development process.

While configuration management may appear to be simply a quality assurance issue rather than a regulatory or technical issue related only to digital I&C, regulatory experience has been that poor configuration management is often a factor that causes significant concerns about the process followed, the products produced and the evidence presented to substantiate safety claims. A software based safety system is formed from many different items of software and hardware, and has many associated documents that provide evidence regarding these items. Hence, it is important that all of the items involved are identified, and have their configuration status established and tracked, so that faults are not introduced due to incorrect versions of these items being used. An effective configuration management system provides the means to ensure this, as well as playing a significant role in a properly managed change control process.

Configuration management remains important throughout the plant life, and can be a particular issue for digital plant upgrades. This concern was discussed in Section 3.3 on management of the functional requirements specification, and also in Ref. [1].

3.4.2. Options

International standards provide a basis for configuration management. IEC 61513 [4] sets some requirements for configuration management. Other standards, such as the International Organization for Standardization (ISO) ISO 10007 [21], the American National Standards Institute (ANSI) ANSI/EIA-649-A [22], IEEE 828 [23], IEEE 829 [24], MIL-HDBK-61A [25], and guidance given in the IAEA-TECDOC-1335 [26] and NRC Regulatory Guide 1.169 [27], describe effective methods of maintaining sufficient configuration management. These standards require the definition of configuration items, basic configuration levels, organization for configuration management and assessment methods for process effectiveness. However, these standards and guidance are not always well known in the nuclear field.

The report on Licensing of Safety Critical Software for Nuclear Reactors [15] presents a number of requirements for Category A software configuration management.

It is a standard practice to include a description of the configuration management in the project or system quality plan, which is reviewed by the customer and any third parties such as regulators.

3.4.3. Associated benefit and challenges

3.4.3.1. Benefit

Good configuration management is fundamental to the delivery and substantiation of nuclear safety systems.

3.4.3.2. Challenges

Experience has shown that superficial configuration management processes often lead to problems in the correct configuration of systems, and consequently in the management of testing and design changes and in the tracing of licensing evidence to source requirements.

3.4.4. Precedent decisions / country experience

Case 1: A system upgrade experienced significant end user changes in requirements all the way through the life cycle, to the point that the functional requirements specification was at revision 26 at the time of factory acceptance testing. This creates a very large workload to maintain configuration control of hardware and software and also a large amount of rework in the development and V&V tasks.

Case 2: An auditor reviewed the software configuration management for a new system and found that software design had proceeded for more than a year, even though there was no approved requirements specification and there were two separate draft requirement documents containing different requirements for the same item. Different drafts were being used by different parts of the project team.

Case 3: An auditor review of the software development process used by the manufacturer of a microprocessor controlled safety system found that the manufacturer had no configuration management document to control the version of software modules installed in devices delivered to the customer.

3.4.5. Recommendations

— Configuration management should be defined at the start of the project.
— Configuration management should be subject to audit.
— Comprehensive regulatory requirements for software configuration management should be established.

3.5. ISSUE No. 5: COMMON CAUSE FAILURE, DIVERSITY AND DEFENCE IN DEPTH

3.5.1. Introduction

3.5.1.1. Defence in depth is fundamental

Defence in depth is generally structured in five levels. Should one level fail, the subsequent level comes into play. The objective of the first level of protection is the prevention of abnormal operation and system failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, in order to prevent or mitigate severe accident conditions that could lead to external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

Implementation of defence in depth usually includes establishment of several successive physical barriers for the confinement of radioactive material. Certain hazards could potentially challenge more than one barrier simultaneously. Such hazards include complex failures of plant systems, such as spurious actuation of safety systems by a fault in an I&C system that affects more than one part of the plant. Generally, design principles, such as single failure tolerance, quality, independence and qualification, provide mitigation for much of the threat for concurrent failure of multiple barriers by applying a number of levels of defence. CCF constitutes the principal threat for compromise of defence in depth. Mitigation of CCF vulnerability is generally accomplished through applications of diversity and defensive design measures.

3.5.1.2. Instrumentation and control can be a challenge to defence in depth

Because I&C systems interact with every system in the plant, I&C systems can be a source of CCF that affects multiple layers of defence in depth. Consequently, special attention must be paid to the plant design I&C system architecture to ensure that the plant can cope with CCF of I&C systems.

Traditionally, I&C system design has included several features to protect the plant defence in depth concept from I&C CCF:

— Separation and functional isolation between control and protection systems to ensure that failures of systems or components will not affect the plant's ability to detect and control abnormal operation or the systems which activate safety features;
— Use of functional and signal diversity within I&C protection systems to cope with the possibility of flawed requirements or the potential that plant parameters, or measurements of parameters, may respond to abnormal conditions or accidents in unpredicted ways;
— Provision of diverse systems or functions in response to CCF experience with certain components (e.g. anticipated transient without scram (ATWS) mitigation systems);
— Provision of safety grade manual system level actuation for safety functions so that operators can always directly initiate safety functions based upon observed plant conditions.

With modern, digital computer based systems, design measures must anticipate additional potential events that were not of significant concern in hardwired analogue systems:

— Individual devices (computers) in modern systems may have a role in implementing many more functions than any single device in traditional analogue systems. Therefore, it is much more likely that failure of a single device can affect multiple functions and potentially challenge more than one level of defence in depth or multiple barriers.
— Latent (i.e. undetected) logical or implementation flaws in software design can be simultaneously triggered by unanticipated conditions when the software is called upon to perform its safety function. This would result in failure of the safety function associated with the fault and could conceivably have indirect effects on other safety functions that are performed in the same component.

3.5.1.3. Acceptance criteria for dealing with common cause failure

Member States use different criteria for determining the adequacy of measures to deal with CCF in protection systems. Some Member States expect the design to include a diverse actuation system (DAS) to back up the plant protection system. Other Member States do not explicitly require a DAS, but do require demonstration that adequate diversity exists.

The provisions that back up the functions of the protection system in the event of CCF may take many forms:

— Inherent safety features (e.g. nuclear characteristics, large coolant inventory and passive safety systems);
— Control system functions that adequately control consequences of anticipated operational occurrences (AOOs) or accident conditions in the event of protection system failure;
— Credit for manual action where operators can be shown to have sufficient time and information to take necessary actions;
— Functional isolation within protection systems such that postulated CCF will still leave sufficient protective functions available;
— DASs that provide necessary protective functions in the event of CCF in the protection system.

Generally, the measures provided in the plant to mitigate the effects of CCF will involve the use of several (and often all) of the above approaches. In general, taking advantage of inherent safety features is the preferred approach. Provision of a separate DAS is often the most expensive approach in terms of both plant cost and operational expense.

Most Member States expect hardwired system manual actuation as one element of the provisions to cope with CCF protection. This hardwired backup control has the capability to maintain the hot shutdown mode during transients. Therefore, the hardwired manual control feature is available as a means to cope with a postulated CCF that could disable the digital protection system. However, an analysis is required to select the number of minimum manual control switches, and the appropriate location should be considered so that these manual features remain accessible to the operator and actuate downstream of the postulated CCF.

While many designers have incorporated DAS into the plant I&C system architectural design, it is not always a given that a DAS is necessary. There have been examples in which regulators have accepted a combination of inherent safety features, control system functions and the possibility of manual actions as being sufficient to deal with the possibility of CCF in the protection system.

3.5.1.4. Adequacy of diversity

There is considerable debate in the industry about what features must be examined to establish evidence that alternative methods of accomplishing safety requirements are not subject to the same CCF.

Where diverse protection is afforded by inherent plant characteristics, the case is often obvious and easily made. By their nature, control systems are functionally diverse from protection systems. The fact that control system functions are different from those of the protection systems often leads directly to signal, functional, design and software diversity between protection and control systems. This is generally more than sufficient to provide high confidence that they are not subject to the same CCF as protection systems. Special attention needs to be given to cases where control and protection functions share common digital components (e.g. microprocessor based motor starters) or signals.

Demonstrating diversity between protection systems and the DAS or diversity within protection systems is more problematic. Generally, the existence of functional diversity and signal diversity are considered strong forms of evidence, but there is a need to confirm that other common features between systems do not jeopardize independence.

3.5.1.5. Classification of diverse actuation systems

Most Member States do not require that systems providing diverse functionality be classified as safety systems. These are generally treated as safety related; however, some designers provide a DAS with redundant architecture to minimize the possibility of spurious trip and to allow for channels to be out of service during operations.

Some Member States strongly prefer that the DAS be ‘hardwired,’ but other Member States place no specific requirements on technology. These Member States instead require justification of diversity between the plant protection system and the DAS. Certainly, the use of hardwired systems simplifies the argument for diversity, but there is no technical basis for presupposing that a computer based DAS cannot be sufficiently diverse from a computer based protection system.

3.5.2. Options

— Regarding mitigation of CCF vulnerability:
  - Provide performance criteria that allow credit for existing plant characteristics and systems (e.g. automatic control, an ATWS system or manual control) as backup to the protection systems, provided that adequate diversity and safety performance can be shown.
  - Provide a separate DAS to act in the event of CCF in the protection system.
  - Incorporate diversity and/or defensive design measures within the protection system to provide internal mitigation of CCF vulnerability.

— Regarding safety classification of the DAS:
  - Apply full requirements for safety systems.
  - Apply requirements for safety related systems.
  - Apply requirements for safety related systems with certain augmented requirements.

— Regarding application of diversity:
  - Continue the subjective, ad hoc approach to applying diversity based on engineering judgement.
  - Establish baseline strategies to guide the selection of diversity combinations.
  - Develop scientifically based measures to enable objective evaluation of the efficacy of different types of diversity in mitigating potential CCF vulnerability.

3.5.3. Associated benefits and challenges

3.5.3.1. Benefits

Regarding mitigation of CCF vulnerability, the first option enables the inherent plant response and designed independence (functional as well as physical) characteristics among I&C systems of different purposes to be leveraged so that additional complexity need not be imposed on the plant I&C system architecture. In many Member States, the regulatory approach accommodates this option as part of an analysis of the diversity and defence in depth characteristics of the plant in response to concurrent CCF and the range of design basis events (see, for example, Ref. [28]).

Where the existing plant characteristics and systems are judged to provide inadequate CCF mitigation, options 2 and 3 serve as prospective approaches to resolving remaining vulnerability. The addition of a DAS enables a separate, independent solution to provide different functions that can back up the vulnerable safety functions. There is a reduced cost if the DAS is not required to be of safety class. Incorporating diversity and defensive design measures within the protection system (e.g. functional diversity in subsystem configurations, diverse measurements of the same parameter or the use of cyclic, invariant software execution loops) may resolve CCF vulnerability within the basic structure of the safety system without requiring introduction of an additional system to complicate the plant I&C system architecture. In addition, this option avoids the potential of spurious actuation of a lower class diverse system (e.g. DAS) that may not include redundancy.

Regarding the safety classification of the DAS, a safety class DAS provides a greater assurance of reliability to avoid spurious actuation and to enhance the expected availability of the system to provide backup functions. A safety related class DAS results in lower costs. A safety related class DAS with augmented quality enhances the expected reliability and availability characteristics of the backup system while retaining some economic benefit over a safety class solution.

Regarding the application of diversity, the first option represents current practice. The second option can expedite design decisions and reduce regulatory uncertainty. The third option would allow for optimized CCF mitigation strategies and improve the understanding of the efficacy of the chosen CCF mitigation (e.g. providing an objective basis for determining what diversity is needed and how much diversity is sufficient).

3.5.3.2. Challenges

The primary challenges for the first option, associated with mitigation of CCF vulnerability, lie in ensuring widespread availability and usage of analysis methodologies as well as consistent determination of the credit that can be given by various regulators. In addition, the methodologies themselves need to be well defined, transparent and amenable to easy interpretation and consistent application. The second option poses challenges associated with the cost of adding and maintaining a separate system, along with the architectural complications introduced by extending the scope and numbers of I&C systems in the plant. In addition, the presence of an alternate, possibly lower safety class, system for performing functions that back up potentially vulnerable safety functions introduces additional responsibilities to any priority logic and may result in spurious actuation of functions that could then challenge or compete with the safety systems. The third option results in a more complex internal structure to the safety system but generally does not significantly alter the higher level safety system architecture (e.g. safety logic replicated in redundant divisions or channels, with the actuation determination processed through a two out of three or two out of four concurrence logic). Options 2 and 3 are each subject to the challenge of demonstrating adequate CCF mitigation (e.g. what diversity is necessary and how much diversity is sufficient). At present, the assessment of CCF mitigation relies on subjective judgements.

The challenge for the options regarding safety classification of a DAS amounts to regulatory practice. Some regulators allow the DAS to be a normal safety related system, while others require some level of augmented quality. In some case histories, the DAS is essentially a secondary safety system qualified to that safety classification. The variation in practice results in regulatory uncertainty, and can lead to vendors having several versions of a DAS to satisfy regulators in different Member States. Obviously, the higher the safety classification, the greater the resulting cost. However, there may be valuable improvements in reliability and availability that are not achieved if a lower safety classification is assigned.

Regarding the application of diversity, the current approach has generally been effective. Nevertheless, the absence of a significant CCF event does not given assurance that the threat has been eliminated. Additionally, the subjective approach may lead to undue complexity that could lead to additional vulnerabilities that have not yet been recognized. Clearly, there is a cost increment associated with each individual diversity incorporated into CCF mitigation strategies. The second option, involving predefined baseline strategies, can help to resolve uncertainty about what mitigation approach might be approved, but it may also lead to more extensive diversity usage and higher cost than is actually necessary. One size fits all approaches tend to impose burdens that could be avoided with more detailed analysis. The third option would help to resolve the concerns expressed here, but the state of the practice and the underlying scientific basis is not yet adequate to enable this capability.

3.5.4. Precedent decisions / country experience

3.5.4.1. Design of diverse features

Historically, diverse features have been incorporated within I&C system architectures to account for potential CCF vulnerability. Specifically, the combination of functional and signal diversity, which are also particularly well suited to provide some level of protection against requirement flaws, have been extensively employed for conventional (i.e. hardwired) safety systems.

Several recent reactor designs have included safety related computer based DASs.

3.5.4.2. Regulatory requirements

The NRC Staff Requirements Memorandum for SECY-93-087 [29] lays out acceptance criteria for coping with potential CCF vulnerability in the protection system. It also specifies relaxed radiological acceptance criteria for diverse actuation. The NRC position is amplified in BTP 7-19 of NUREG-0800, Chapter 7 [30], which provides review guidance for safety systems to NRC staff. The approach to conducting the required diversity and defence in depth analysis is documented in NUREG/CR-6303 [28], and further clarification of CCF mitigation strategies is provided in NUREG/CR-7007 [31]. In NUREG/CR-7007, the NRC research identified three primary strategies of diversity usage in accordance with differences in technologies that serve as the basis for diverse systems, redundancies or subsystems. These strategies involve: (a) fundamentally diverse technologies (e.g. analogue and digital implementations), (b) distinctly different technology approaches (e.g. different digital technologies such as the distinct approaches represented by programmable logic devices and general purpose microprocessors) and (c) architectural variations within a technology (e.g. different digital architectures such as the diverse microarchitectures provided by different central processing units).

In recent years, the Western European Nuclear Regulators' Association engaged European safety authorities to establish a common position on the licensing of safety critical software. The common position of the European regulators [15] consists of consensus requirements (based on unanimous agreement) and recommended practices (based on general agreement) addressing key licensing considerations. The common position requires that "principles of redundancy, diversity, physical isolation, segregation, and separation between safety functions, safety related functions and functions not important to safety" be applied to computer system architecture design. These principles address considerations such as reliability and independence while providing protection against CCF.

The common position on software design diversity addresses design decisions (i.e. diversity seeking decisions (DSDs)) that invoke methods, techniques and measures to force software design diversity. The goal is to diversify failure behaviour among diverse software based systems. Functional diversity is the foremost DSD identified in the common position, and it is required to be implemented whenever possible for safety system elements that are intended to be diverse. Additionally, functionally diverse systems are required to be associated with the same safety

class and subject to the same graded requirements. It is noted that the adoption of a simple hardwired system as the diverse alternative to a computer based safety system can resolve software related CCF concerns, and this approach is emphasized as a best practice recommendation for this topic.

3.5.4.3. Consensus standard requirements

IEC Subcommittee 45A has responsibility for standards that apply to I&C systems important to safety in nuclear power plants. The IEC standard that covers the system aspects of I&C systems important to safety is IEC 61513 [4]. The standard requires an "evaluation of the effectiveness of measures used to reduce the sensitivity of the safety groups to CCF", with an emphasis on Category A (i.e. safety) functions. Correspondingly, the standard requires the provision of "measures against the occurrence of a CCF within I&C systems implementing different lines of defence against the same PIE."

IEC 62340 [32] provides a framework for establishing a CCF coping strategy that is consistent with the high level requirements in IEC 61513 [4]. Specifically, IEC 62340 gives requirements regarding the avoidance and mitigation of CCF and provides principles to promote independence among I&C systems. The use of functional (and the supporting signal) diversity is central to the guidance provided by the standard.

3.5.4.4. Nuclear and non-nuclear experience

The treatment of CCF vulnerability in non-nuclear industries varies from no diversity (e.g. the almost total reliance on redundancy of high quality modules and defence in depth layers with no 'intentional' diversity), to minimal diversity (e.g. reduced functionality backups with limited diversity), to more extensive diversity (e.g. combinations of techniques for fault management addressing high consequence failures with 'encouraged', but not fully specified, diversity).

Based on nuclear power experience, a common diversity usage approach by the industry involves a systematic subdivision of the protection functions into different systems or subsystems and an assessment of the degree of diversity between the two versions based on a pairwise comparison of the individual mitigation characteristics. Based on a study of case histories [31], the approaches to diversity usage can be grouped into three broad categories: coequal diverse systems, primary/secondary diverse systems and functionally diverse subsystems. The use of a DAS would correspond to the second category.

An investigation of CCF mitigation strategies providing examples from both nuclear and non-nuclear industries is documented in NUREG/CR-7007 [31].

Additional considerations regarding CCF vulnerability and the efficacy of mitigation techniques are described in IAEA NP-T-1.5 [33].

3.5.5. Recommendations

- Member States will ideally clearly establish common requirements and acceptance criteria for defence against CCF within protection systems. Ideally, these would be performance based, similar to the criteria given in the NRC Staff Requirements Memorandum for SECY-93-087 [29], BTP 7-19 [30] and European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 10: Instrumentation and Control and Man-Machine Interface [34].
- Developers of new I&C systems (either for new design or operating plant upgrades) should develop a strategy for coping with protection system CCF early in the system design and should take full advantage of inherent plant safety characteristics, control system capabilities and operator capabilities. Consideration should be given to designing the protection systems with sufficient internal diversity to cope with a range of possible CCF.
- Where a DAS is provided, it does not need to back up all functions of the protection systems — only those for which adequate protection against CCF cannot otherwise be shown.
- Demonstration of signal diversity, equipment diversity and functional diversity between the DAS and protection systems will usually be necessary to establish that the two systems are not subject to the same CCF.

— It should not be generally necessary to build a DAS to the full set of requirements that are applied to safety systems. It would be appropriate to pay more careful attention to certain attributes such as the extent of functional and environmental qualifications. Construction in accordance with criteria such as those recommend by IEC 61226 [35] for Category 2 systems seems sufficient.

3.6. ISSUE No. 6: USE OF SMART DEVICES

3.6.1. Introduction

Smart devices are devices such as sensors and valve actuators that contain computer based technologies and are configurable to make them suitable for a variety of applications. Smart devices are displacing traditional analogue sensors and actuators in many industrial applications as they can offer a significant number of benefits such as improved stability, self-diagnostics and additional features. This displacement is likely to result in some traditional analogue devices becoming obsolete, and not being available for use in the nuclear industry. Smart devices have been considered difficult to qualify in the nuclear industry owing to detailed design information not being readily available as a result of proprietary considerations around the embedded functions. Smart device reliability is generally dominated by systematic concerns caused by the use of computer based technologies. This creates a challenge where traditional analogue instruments are no longer available, and there is uncertainty as to how potential smart device replacements are to be qualified for use in the nuclear industry.

3.6.2. Options

— Avoid using smart devices and support the continued production of nuclear grade analogue devices. Accept that the potential benefits of smart devices cannot be realized in the nuclear industry.
— Develop approaches to the qualification of smart devices for nuclear safety applications that are acceptable to regulators and nuclear power plant operators.

3.6.3. Associated benefits and challenges

3.6.3.1. Benefits

Smart devices enable additional information to be gathered such as the status of the smart device and its instrument channel, any loss of accuracy or incipient failures, and so on. This enables early decisions to be made regarding ongoing operation and any safety actions required. Smart devices can provide additional functions that may be beneficial such as readout in selected engineering units, local readouts, signal validation and processing, alarm output when a threshold is reached, and so on.

3.6.3.2. Challenges

It may be difficult to identify that smart devices have been incorporated into packaged equipment performing a nuclear safety function. It is thus necessary to identify whether a smart device is present in replacement equipment, components and systems, and to qualify any smart device accordingly.

Smart devices have to be configured to operate as intended. Thus, any misconfiguration has the potential to compromise the intended function of the device. Misconfiguration could arise from a fault within the smart device (e.g. memory loss or software fault), unintended reconfiguration or fault in a device being used to set the configuration. Some smart devices may be configured by buttons on the device itself, and unauthorized reconfiguration may need to be prevented by suitable means.

A smart device will generally contain features that are not used for a given application, and these additional features have the potential to interfere with features that are being used. Therefore, measures need to be taken to ensure the quality of the software in particular, and avoid unintended consequences of additional features. This is often difficult because smart device manufacturers do not wish to reveal commercially sensitive design information.

Where the same type of smart device is used in redundant channels there is the potential for CCF to result in the simultaneous failure of all channels on which the device is present. Where the same type of smart device is used in more than one layer of protection, there is the potential for CCF to result in the simultaneous failure of more than one layer of protection.

3.6.3.3. Safety classification

It is necessary to ensure that a smart device has sufficient reliability for the application, including hardware and software, and for the systematic aspects of the design, such as the interaction between the software and hardware, to be considered. This is challenging where design information is not available.

3.6.4. Precedent decisions / country experience

In the UK, the Control and Instrumentation Nuclear Industry Forum has undertaken research into the qualification of smart devices and has produced a tool, 'Emphasis', which may be used to provide evidence for the production excellence aspect of smart device qualification. This tool consists of a structured question set based on IEC 61508 [3] requirements that enables a reviewer to decide whether the device meets a particular requirement. Evidence can be recorded against each requirement to allow a demonstration of adequacy to be made. Independent confidence building measures such as static analysis, according to the intended device classification, are also required. This approach has been successfully used to qualify smart devices for use in nuclear safety applications in the UK.

3.6.5. Recommendations

— Smart devices should be considered where they provide nuclear safety benefits.
— Smart devices are complex devices with a range of potential failure modes, and qualification should include an assessment of the potential consequences of these failure modes, and the adequacy of measures to protect against them.

3.7. ISSUE No. 7: SAFETY CLASSIFICATION SCHEMES

3.7.1. Introduction

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 of 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.

The safety classification approaches used in nuclear power plants are based on the safety philosophy and the plant design basis. All structures, systems and components (SSCs), including software for digital I&C systems, are classified on the basis of their function and significance with regard to safety. SSCs, including software for digital I&C systems installed and used in order to cope with PIEs, are assigned to the highest safety class, while less important functions and equipment are allocated to lower safety classes. In safety classification, there are also principles by which the safety class is inherited by auxiliary systems from the systems they support. The safety classifications used in nuclear power plants are defined by standards such as IEC 61226 [35], IAEA NS-G-1.3 [36] and IEEE 603 [37], and in national regulations.

In each safety classification approach, there are technical and design requirements defined for each safety class. The requirements are more relaxed for lower class systems. Following this principle, SSCs, including software for digital I&C systems, are designed such that their quality and reliability are commensurate with their safety class. 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 should be as simple and analysable as possible. Another design principle is to make sure that any failure in a system belonging to a lower class will not propagate to a higher class system. Following these design principles facilitates the licensing process. It is also important that the technical and design principles tied to each safety class are generally understood by the licensee and the regulator before the design is started.

Table 1 provides an overview of the different classification schemes implemented in different regulatory regimes and consensus standards. The table is a comparison of the schemes applied to I&C systems within the international nuclear community.

TABLE 1. SAFETY CLASSIFICATION SCHEMES APPLIED TO INSTRUMENTATION AND CONTROL SYSTEMS

Standard	Classification of the importance to safety				
	Systems important to safety				Systems not important to safety
IAEA NS-R-1	Safety		Safety related		Systems not important to safety
International Electrotechnical Commission 61226 Functions Systems	Category A Class 1	Category B Class 2	Category C Class 3		Unclassified
Canada	Category 1		Category 2	Category 3	Category 4
France N4	1E	2E	SH	Important to safety	Systems not important to safety
European Utility Requirements	F1A (automatic)	F1B (automatic and manual)	F2		Unclassified
Japan	PS1/MS1		PS2/MS2	PS3/MS3	Non-nuclear safety
Republic of Korea	IC-I		IC-II		IC-III
Russian Federation, Ukraine	Class 2		Class 3		Class 4 (systems not important to safety)
Switzerland	Category A		Category B	Category C	Not important to safety
UK Functions Systems	Category A Class 1	Category B Class 2	Category C Class 3		Unclassified
USA	Systems important to safety				Non-nuclear safety
	Safety related, safety or Class 1E		(No name assigned)		

In each country, there are requirements and conventions that define how the I&C systems in each class should be designed and implemented. Typically, requirements are set for products and for work processes. Associated with each class, there may be requirements that relate to the licensing process and the evidence to be presented. A common safety philosophy is the most important prerequisite for harmonization. Agreement of a common classification approach might appear to be straightforward, but practice has shown that it is often difficult to achieve.

Currently, there appears to be reasonable agreement on the requirements for the most demanding safety classes. However, there seems to be less of a consensus on how these requirements may be relaxed in the lower safety classes. Additional clarifications may therefore be more necessary in the lower safety classes to achieve improved harmonization. Historically, for electrical and I&C equipment in the USA, the classification has been either Class 1E or non-Class-1E. However, it has been recognized in both international and US regulatory practice and industry standards that this approach is problematic. The policy of one vendor is to follow a three tiered classification system for I&C systems, which meets the intent of international [35, 38] and US [39, 40] requirements.

The various codes and standards that guide classification of SSCs are inconsistent in the approach and terminology they apply to the topic of I&C classification. The term 'safety related' has two different meanings in the USA and international regulatory arenas. The term 'important to safety' is similarly conflicted. A practical approach to classification is needed that can be tailored to meet the needs of specific projects while at the same time enabling the standardization of processes with regard to meeting requirements imposed by classification.

The Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group is endeavouring to identify opportunities for converging applicable standards and regulatory practices among MDEP countries. This effort is in accordance with the Terms of Reference for the Issue Specific Working Groups as well as the objectives of the MDEP. Convergence is possible only where there is agreement on overriding principles and positions.

In the area of safety classification, all nations accept the principle that functions and SSCs should be classified according to their safety significance. Unfortunately, there are a multitude of different categorization schemes. These schemes not only use different criteria for determining safety significance, they also use different, and sometimes conflicting, terminology. This situation makes convergence difficult or impossible, except in areas where the question of classification can be avoided.

The diversity of safety classification schemes slows the introduction of digital I&C technology, inhibits common ground in important areas and obstructs harmonization of standards between standards organizations that reference different schemes. Classification is an important issue, but the question of safety classification cannot be resolved solely within the I&C community.

Requirements for classification, based on the importance of functions to achieving safety, are introduced in SSR-2/1, Safety of Nuclear Power Plants: Design [38], and NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants [36]. SSR-2/1 [38] describes items important to safety as SSCs that are part of the assembly of equipment designated to perform all actions required for a particular PIE to ensure that the limits specified in the design basis for AOOs and design basis accidents are not exceeded.

IEC 61226, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Classification of Instrumentation and Control Functions [35], is based on the general requirements of the IAEA publications, and divides functions important to safety into three categories: A, B and C. IEC 61513, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — General Requirements for Systems [4], introduces the concept of equipment classes to draw a distinction between the categorization of functions important to safety and the identification of the systems that perform those functions. Table 2, from IEC 61513 [4], shows the relationship between categories and classes.

3.7.1.1. Types of functions significant to safety

The system classification process begins with the enumeration of functions that have some significance to plant safety. These functions are categorized according to the degree of significance to safety or plant availability. These functions are then allocated to systems and equipment of a given class depending on the category of the function.

TABLE 2. CORRELATION BETWEEN CLASSES OF I&C SYSTEMS AND CATEGORIES OF I&C FUNCTIONS

Categories of I&C functions important to safety			Corresponding classes of I&C systems important to safety
A	(B)	(C)	1
	B	(C)	2
		C	3

Note: I&C functions of Category A may be implemented in Class 1 systems only, I&C functions of Category B may be implemented in Class 1 and 2 systems, and I&C functions of Category C may be implemented in Class 1, 2 and 3 systems.

The determination of the safety significance of a given function takes into consideration factors such as:

— The safety function(s) to be performed;
— The role of the function in preventing or mitigating PIEs;
— The role of the function during all operating modes (e.g. startup or normal operation refuelling);
— The role of the function following PIEs such as natural events (e.g. seismic disturbance, flood, extreme wind or lightning) and internal hazards (e.g. fire, internal flood, missiles, radioactive release from adjacent unit or chemical releases from other plants or industries);
— The consequences of failure of the I&C functions;
— The effects of spurious actuation of the I&C functions;
— The probability that it will be required to perform a function significant to safety;
— The time following a PIE at which, or during which, it will be required to operate;
— The maintenance, repair and testing strategy.

IAEA NS-G-1.3 [36] describes four types of I&C functions that are important to safety in the terminology of that publication. The requirements for assurance of these functions depend upon their types as well as the level of importance to safety.

Protection functions

Protection functions provide a line of defence against failure in other plant systems. They are among the most critical of the safety functions and relate directly to nuclear safety in terms of protecting personnel and the public in the event of a serious failure.

Control functions

Control functions provide assurance that the plant is controlled and kept within its operating envelope under normal and abnormal conditions. Control functions can also mitigate the effect of plant transients or PIEs, thereby contributing to nuclear safety by minimizing the demand on protection functions.

Monitoring and display functions

Monitoring and display functions provide the interface between the plant and the operations and maintenance personnel. These functions are significant to safety as they allow plant personnel to intercept transients and maintain the plant within the envelope for safe operation.

Testing functions

Testing functions provide assurance of the availability and effectiveness of other functions significant to safety, and confirm that these have not been degraded.

3.7.1.2. Function categorization

The approach to classification normally starts with the categorization of the functions to be performed by I&C systems, which are assigned to categories according to their importance to safety. The safety importance of a function is related to the consequences if the function fails when it is required to be performed and also to the consequences in the event of a spurious actuation. The category of the function determines the classification, and hence the design and quality requirements, for the I&C systems and equipment. An example of this approach is provided by IEC 61226 [35] and its three safety categories.

Category A denotes the functions that play a principal role in the achievement or maintenance of nuclear power plant safety to prevent PIEs from leading to unacceptable consequences. This role is essential at the beginning of the transient when no alternative actions can be taken, even if hidden faults can be detected. These functions are required to achieve the stabilization of the transient, which corresponds to a controlled state of the plant, where the reactor is subcritical, the heat removal is ensured and radioactive releases are limited. If specified manual actions are provided to reach a stable state, factors such as the availability of redundant information sources, sufficient duration of the grace time for operator evaluation of alternative sources of information, and whether the manual actions are the only possibility for mitigation of this sequence of events to preserve nuclear power plant safety have to be considered.

Typical I&C systems performing Category A functions are:

— RPSs;
— Safety actuation system and safety system support features;
— Key instrumentation and displays to permit preplanned operator actions that are required to ensure nuclear power plant safety.

IEC 61226 [35] provides further details of the criteria it proposes for functions to be assigned to each of the different categories: Category A functions shall only be implemented in Class 1 systems.

Category B denotes functions that play a complementary role to the Category A functions in the achievement or maintenance of nuclear power plant safety, especially the functions required to operate after a stable state has been achieved, to prevent a PIE from leading to unacceptable consequences, or mitigate the consequences of a PIE. The operation of a Category B function may avoid the need to initiate a Category A function. Category B functions may improve or complement the execution of a Category A function in mitigating the consequences of a PIE, so that plant or equipment damage or release of radioactive material may be avoided or minimized.

Category B also denotes functions whose failure could initiate a PIE or worsen the severity of a PIE. Because of the presence of a Category A function to provide the ultimate prevention of or mitigation of the consequences of a PIE, the safety requirements for the Category B function need not be as high as those for the Category A function.

Typical I&C systems performing Category B functions are:

— Nuclear power plant automatic control systems;
— Parts of the decay heat transport to ultimate heat sink systems that are not necessary in the short term;
— Instrumentation needed to apply operating procedures for design basis events;
— Safety circuits and interlocks of fuel handling systems used when the reactor is shut down.

Category B functions are implemented in Class 2 or Class 1 systems. In some countries, the classification may be upgraded if the system is required to remain operable during and following a seismic event.

Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of nuclear power plant safety. Category C includes functions that have some safety significance, but are not Category A or Category B. They can be part of the total response to a PIE, but may not be directly involved in mitigating the physical consequences of the accident, or functions necessary for beyond design basis accidents.

Examples of such functions could be:

— Access control functions;
— Operator displays and alarms;
— Plant computer functions.

Functions that do not play any role in the achievement of nuclear power plant safety are uncategorized and are designated as not important to safety [38] or unclassified [35]. Such functions may be implemented on general non-safety classified equipment.

3.7.1.3. Evolution of the safety classification

The safety classification issues presented above are based on existing plant designs and the current state of technology of I&C systems. For new generations of plant designs and advanced I&C technology, the above classification may change, but it is expected to follow the spirit of the SSC classification discussed above.

There are numerous examples of differences in the safety classification between generation II, III and III+ designs. The introduction of passive plant design and fully computerized control rooms are two of the examples that may change mapping of I&C systems to different categories and SSC classes.

3.7.2. Options

— Continue country specific application of safety classification with associated gaps between the two main classification schemes:
  • IEC — Europe — three safety categories: A, B and C, and a non-safety category;
  • IEEE — NRC two classes: 1E / safety related and non-1E / non-safety-related;
— Develop a harmonized, global classification system including quality classes.

An example of one such exercise being undertaken is an IAEA publication [41] for the safety classification of SSCs in nuclear power plants. It is possible that a scheme such as this could be used in the future as the basis for developing a harmonized, global classification scheme.

3.7.3. Associated benefits and challenges

3.7.3.1. Benefits

— Minimize costs/time involved in supporting multiple classification systems.
— Reduce the barriers that make it difficult to use systems and equipment developed under one classification scheme on nuclear power plants operating under a different classification scheme.

3.7.3.2. Challenges

Gaining acceptance for one method of classification by regulators, and associated standards endorsement.

3.7.4. Precedent decisions / country experience

Safety classification is affected by the specific country law. A challenging situation may occur where a new nuclear power plant construction follows the vendor’s own classification system, which conflicts with country practices.

3.7.5. Recommendations

An internationally accepted approach to safety classification is needed. Activities to establish international guidance for safety classification are ongoing within both the MDEP and the IAEA. Both of the activities are important, and should be supported by industry.

3.8. ISSUE No. 8: COMPUTER SECURITY

3.8.1. Introduction

As nuclear facilities modernize digital I&C systems, attention to computer security has intensified as clear and recurring proofs of the vulnerabilities of computer systems come to light. Malicious exploitation of these vulnerabilities has been witnessed with growing frequency and impact.

Possible cyber-attacks could be associated with business espionage, technology theft, a disgruntled employee, a recreational hacker, a cyberactivist, organized crime, a nation State or a terrorist organization.

The possible occurrences of cyberterrorism as a means of attacking a Member State's critical infrastructure have prompted a number of national authorities to prepare defences and issue new regulations. These cover computers used in safety and safety related systems, which should be protected from possible cyber-attacks, and also computers used to control and monitor the plant.

Additionally, requirements to protect safety systems from computer security attacks and separate requirements to maintain continuity of power during cyber-attacks are being promulgated at the same time. These provide conflicting guidance that has not yet been resolved in many cases.

The nuclear industry needs specific guidance in computer security requirements for digital I&C systems including well defined approaches and acceptance criteria. This is necessary to minimize the impact of costly delays, vulnerabilities of attack and varying regulatory positions across country boundaries.

The development process for digital I&C systems should address potential security vulnerabilities systematically at each stage of the life cycle to meet the confidentiality, integrity and availability requirements. Safety and safety related computers executing critical applications, control and monitoring computers for power production, as well as computers that store important and sensitive data, have to be protected to ensure that data are not erased, stolen or otherwise manipulated for a malicious purpose.

Experience gained from fields such as the military, national security, banking, electricity distribution and air traffic control is valuable for improving computer security at nuclear power plants with digital I&C systems. In particular, in the information technology field, information security has itself evolved rapidly, creating a rich set of international best practices and standard documents (e.g. the ISO/IEC 27000 series [42]).

Computer security should now be a part of the overall security programme at a plant. The tools for identifying threats, assessing the security positions and building barriers include technical tools, such as intrusion detection, virus scanners, firewalls and encryption, as well as administrative tools, such as the application of security zones, security management systems and access control (i.e. passwords and biometric identification). For critical systems, where high security is needed, a unidirectional device (e.g. a data diode or an opto-isolator) should be considered as a possible solution. This solution can ensure the integrity and availability of the system by preventing data modification or changing the operation of a nuclear power plant. Network intrusion detection system or host based intrusion detection system strategies (or both) were developed to comply with requirements from Regulatory Guide 5.71 [43], and NEI 08-09 (Appendix D) [44].

Development and implementation of a computer security programme plan includes the performance of an overall risk assessment. This risk assessment document:

— Defines the scope of the security risk assessment for each system;
— Identifies the key threat groups and the security risks associated with them;
— Provides a risk management summary of the security requirements to manage each risk, the security relevant properties of the design and the implementation of countermeasures.

One security architecture that serves as an example is based on Regulatory Guide 5.71 [43], and is outlined in Fig. 1. The defensive architecture provided in Fig. 1 includes a series of concentric defensive levels of increasing security.

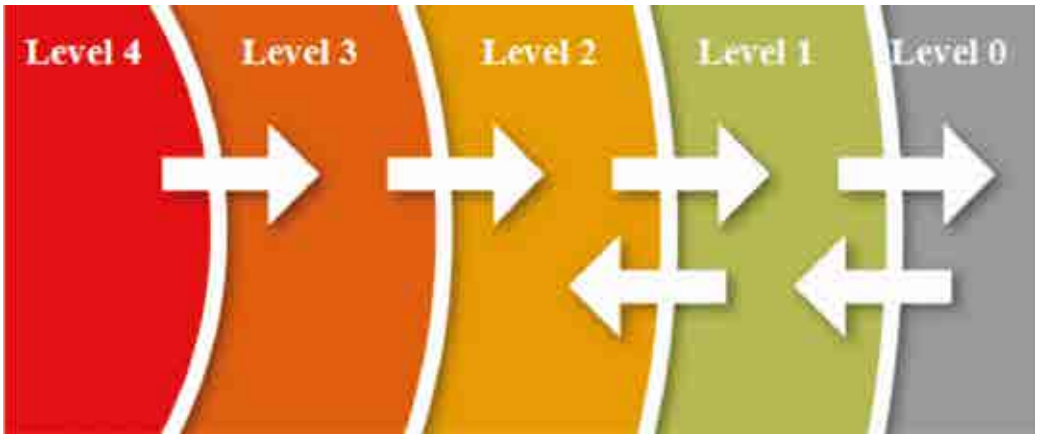


FIG. 1. Simplified computer security defensive architecture.

The security architecture involves establishing multiple security boundaries as part of a defence in depth strategy designed to protect critical digital assets (CDAs) and networks from cyber-attacks. In this way, multiple mechanism protection levels must fail for a cyber-attack to progress and impact a critical system or network. Defence in depth is achieved by:

— Implementing multiple security boundaries;
— Instituting and maintaining a robust security control programme that assesses, protects, responds to, prevents, detects, mitigates and recovers from an attack on a CDA.

CDAs associated with safety, safety related and security functions — as well as support systems and equipment that, if compromised, would adversely affect safety, safety related and security functions — are allocated to level 4, and are protected from all lower levels. Only one-way data flow is allowed from level 4 to level 3, and from level 3 to level 2. Initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited. Data only flows from one level to other levels through a device (or devices) that enforce(s) the security policy between each level.

Interfaces between level 4 CDAs and systems at lower security levels should be secured via the implementation of a unidirectional (cut wire) gateway. This control will establish a hard barrier that isolates level 4 systems from external access. Remote access to level 4 systems should not be permitted.

A firewall based level 3/2 ‘demilitarized zone’ (DMZ) will house systems that are not CDAs based on safety, security and emergency preparedness functions requiring data from the level 4 CDAs. Communication will flow from level 4 to the systems via the cut wire gateway. These systems may be accessed by level 2 systems.

Security monitoring systems at level 4 provide data to the level 3/2 DMZ security monitoring system via the cut wire gateway. Centralized monitoring is consolidated within the level 3/2 DMZ. Security related alarms are monitored within level 4 and alarmed via relay to site security.

The development of regulations, guidance and standards to maintain computer security is evolving. Computer security vulnerability might be significantly reduced if such regulations, guidance and standards are followed rigorously and if computer security programmes for new systems and plants are developed.

In addition, the issues of computer security for nuclear plants extend beyond consideration of the safety systems into consideration of non-safety systems that provide control and indication functions. This challenges the vendor, end user and regulator with the issue of extending the regulatory umbrella to non-safety systems for this subject matter.

3.8.2. Options

— Member States continue to develop their own specific regulations to address protection of critical assets including nuclear plants. Examples include:
  • NRC Regulatory Guide 5.71 [43];
  • NEI 08-09, Revision 6 [44];
  • US 10 CFR 73.54 [45];
  • NRC Regulatory Guide 1.152, Revision 3 [46].
— Member States agree on a common set of guidance and standards, including acceptance criteria to address cyber-security and computer security concerns. This set includes the following:
  • IAEA guidelines on computer security [47];
  • IEC standard 62645 on computer security [48];
  • Other internationally accepted standards and guidelines.

3.8.3. Associated benefits and challenges

3.8.3.1. Benefits

— Protect the systems and equipment from cyber-attacks so that they can perform their intended safety functions;
— Protect the non-safety systems from cyber-attacks so that they may maintain control and indication for continuity of power.

3.8.3.2. Challenges

— Lack of direction in this area may result in vulnerability to attack. In addition, improper application of guidance from other application domains to nuclear power safety and control could impose measures that affect safety and operability.
— Confidentiality of cyber-designs and test results are not transparent, which inhibits progress in the development of the design criteria in this area.

3.8.4. Precedent decisions / country experience

In the Republic of Korea, KINS has been developing a regulatory guide on cyber-security of digitalized I&C systems that aims at preventing, detecting and responding to malicious acts involving nuclear and other radioactive materials and associated facilities. The guidance covers technical and managerial controls for the computer security of safety I&C systems. This guidance focuses on ensuring the safety of nuclear facilities, which means the target systems of computer security activities are safety I&C systems and equipment.

KINS has regulatory experience for new plants in the Republic of Korea; specifically, Shin-Kori units 3 and 4 and Shin-Ulchin units 1 and 2. KINS requested the licensee to establish and submit their plans for cyber-security activities prior to the application of the operating limits of the plants. The tentative framework of those plans is categorized with administrative, managerial and technical strategies.

Other experience is related to a review of the topical report on large scale digitalized I&C system development, under the Korea Nuclear I&C System project. KINS requested the applicant to establish and submit the result of cyber-security activities for the development of programmable logic controller based control and RPSs. The applicant carried out the cyber-security assessment. KINS reviewed the cyber-security policy document, the overall plans and the results of penetration testing, amongst others.

KINS also contributed to the development of the IAEA publication, Computer Security at Nuclear Facilities [47]. As there are rapid changes to digital technologies, computer security is one of the challenges still ‘pushing security’. This is why international cooperation is needed to resolve this issue properly.

The Oconee Nuclear Station RPS / engineered safety features actuation system (ESFAS) digital upgrade was evaluated by the NRC for conformance to computer security requirements, following the guidance in NRC Regulatory Guide 1.152, Revision 2 [49]. This regulatory guide [49] utilizes waterfall life cycle phases as a framework for describing specific digital safety system security guidance and for establishing criteria for

acceptability. The Oconee RPS/engineered safeguards protective system (ESPS) digital upgrade was evaluated by the NRC for computer security controls against those criteria for the identified life cycle phases, which consist of the following phases:

— Concepts;
— Requirements;
— Design;
— Implementation;
— Test.

Details on the results of the review are included in Ref. [10].

3.8.5. Recommendations

There is a need for high level guidance relevant to computer security for systems important to safety at nuclear power plants. This would provide principles as a basis for standards organizations to develop detailed guidance. In parallel, it is expected that regulators will be assessing submitted designs and setting precedents in this area.

3.9. ISSUE No. 9: HARMONIZATION OF STANDARDS

3.9.1. Introduction

The introduction of new (e.g. digital) I&C technology in nuclear power plants has led to the revision of many standards and guidelines and the development of several new ones. The IAEA has been active in this area over the years, and several standards, technical reports and guides have been published at different levels of focus, ranging from specific topics or particular systems to broad issues or overall I&C system architectures. International standards organizations such as the IEC, the ISO, the IEEE and the International Society for Automation (ISA) are primarily responsible for producing and maintaining standards. This work is ongoing, with the development of important new standards and the revision of old standards as continuing processes.

These standards organizations begin work from the same safety fundamentals and have similar goals, but the standards that they develop are not necessarily structured according to specific organization formatting principles, which complicates demonstration of equivalence. Of more significance, the comparable standards from different organizations often contain varying degrees of difference in technical details. National licensing authorities have, to some extent, incorporated available standards in their requirements and guidance, but they have also produced their own requirements and guidelines. This process of tailored endorsement enables emerging issues and challenges in the application of new technology to be addressed, but also introduces treatment of specific national concerns. Consequently, there are differences in national licensing requirements for digital I&C. These differences do not lead to significant differences in safety, but do create significant differences in the details of how the safety case is made for I&C systems. These differences have sometimes made the application of the new technology for international usage difficult or more expensive. For example, one issue to resolve has been how specific solutions that have been created within one system of standards could be evaluated in another system. In refurbishment projects, nuclear utilities have sometimes found it difficult to establish and argue for the use of a specific set of requirements. Experience has shown that vendors can have difficulties trying to interpret and address the variations between national requirements and different sets of comparable standards. Finally, there have also been cases where national licensing authorities have found it challenging to manage the assessment of a variety of technical solutions based on different guidelines and national/organization conventions in the context of their own regulatory regime.

An obstacle to standards harmonization is that standards development organizations must respect the regulatory framework that they support. By agreement with the IAEA, the IEC Nuclear Power I&C Subcommittee provides guidance for the implementation of IAEA safety requirements and takes the IAEA publication NS-G-1.3 [36] as the principal guidance. There is no formal position on the reference regulations for IEEE nuclear standards, but most IEEE standards take the NRC regulations as a starting point. The differences between the IAEA and NRC criteria thus influence each organization's standards, and these differences will sometimes complicate, or even

preclude, full harmonization. Ultimately, standards cannot be fully harmonized as long as the various national and international requirements documents have significant differences in detail.

Software V&V is one example of an area where differences between guidance of various standards cause trouble. Here, there are three sets of widely used standards: IEC 60880 [50] and 62138 [51], IAEA NS-G 1.1 [14] and IEEE 1074-2006 [52], and IEEE 7-4.3.2-2003 [8] and IEEE 1012 [11]. The IEEE and IEC standards take fundamentally different approaches to the problem. Both approaches are sound, but reviewing a design developed using IEEE 1012 [11] against criteria based on the guidance of IEC 60880 [50] is problematic. Even where fundamentally different approaches are not taken, differences in detail can cause considerable complexity and extra expense, with the effort expended yielding no discernible improvement in safety.

Examples of other overlapping standards where the different guidance results in unnecessary effort include:

— Environmental qualification: IEC 60780 [53] and IEEE 323 [54];
— Seismic qualification: IEC 60980 [55] and IEEE 344-2004 [56];
— Surveillance testing: IEC 60671 [7] and IEEE 338-2000 [57].

Development of harmonized standards is only a first step. Even in the presence of harmonized standards, different regulatory authorities may apply the standards in different ways during a review. For example, standards agree that there should be a set of V&V activities that are conducted independent of developers and which give independence criteria that must be met. No standards require that IV&V be implemented by a third party organization. Nevertheless, some regulatory authorities or utilities require third party IV&V, and some do not.

Therefore, even when standards are well harmonized, regulatory authorities should develop common positions on the interpretation of standards. The Nuclear Energy Agency MDEP Digital Instrumentation and Control Working Group is endeavouring to develop such common positions in certain areas. It is not enough, though, to just document a common view. To be effective, these common views would need to be incorporated into the reviewer guidance and practices of each regulatory body. Furthermore, coordination between regulators must continue indefinitely to ensure consistency among regulatory practices is maintained as situations change and standards evolve.

Even if processes for harmonizing standards are well established, standards harmonization cannot resolve every issue. Standards development is a slow process. It takes time to achieve consensus among a large group, and the individuals who develop standards need time to gain experience with new technology before best practices can be identified. Consequently, I&C projects in progress may have to apply guides and standards that are still in draft form or synthesize their own guidance when suitable guidance documents are not yet available. In situations where there are no harmonized guidance 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 that arises is thus not the absence of guidance, but rather deciding on what guidance to apply and how it should be used. An additional challenge is that standards organizations can only develop requirements and guidance to a certain level of detail. Thus, the vendor must still interpret and implement the guidance, and the regulator must assess the available evidence to determine whether acceptable compliance with the standard has been achieved.

A challenge to vendors is the requirement to meet so many different standards when developing and qualifying equipment. The qualification efforts alone can require that a vendor have two separate qualification processes to meet the different standards. This adds additional cost, and provides supply chain challenges as well as quality challenges. One set of harmonized standards would reduce this effort and risk, and would also make it much easier for the operators and regulators to review the testing performed.

3.9.2. Options

— Maintain separate consensus standards for safety related nuclear power applications to be adopted by Member States in varying methods and to varying degrees.
— Establish a harmonized set of standards applicable to safety related nuclear power applications widely adopted by the national regulators of the IAEA Member States.
— Establish review practices that can accept alternative methods that demonstrate the safety goal has been achieved. As an example, IEC 60880 [50] and IEEE 1074-2006 [52] both provide guidance to develop safety software, but use different approaches to achieve the same result.

These options are not mutually exclusive. It is likely that the best solution for certain standards will be the first option, for others, the second option and, for still others, the third option.

3.9.3. Associated benefit and challenge

3.9.3.1. Benefit

The availability of broadly accepted harmonized standards can reduce the cost for establishing compliance of existing or new digital equipment to Member State requirements.

3.9.3.2. Challenge

Gaining acceptance by the standards organizations and regulators of one set of harmonized standards for all safety related applications in nuclear plants and facilities.

3.9.4. Precedent decisions / country experience

Currently, certain dual logo standards (IEC and IEEE) are in progress, with more under evaluation. The MDEP Digital Instrumentation and Control Working Group is making an effort to identify the most important inconsistencies between standards and to develop common positions among ten regulators to deal with these inconsistencies.

3.9.5. Recommendations

— Standards organizations should try to produce identical guidance where this is possible (e.g. joint logo standards).
— Where identical guidance is not possible, the various standards organizations should interact to minimize the prospect of contradictory requirements.
— Where a standards organization decides it is necessary to issue guidance that is contradictory to the guidance of another standards organization, it should document the reasons why this is necessary. The possibility of resolving this contradiction should be evaluated.
— Regulators should work to achieve a common application of harmonized standards.
— In some cases where standards offer different approaches to achieving the same safety goal, regulators should work together to establish a common position on the acceptability of either approach.

3.10. ISSUE No. 10: TAKING CREDIT FOR ON-LINE MONITORING

3.10.1. Introduction

On-line condition monitoring of instrument channels, plant equipment, systems and processes includes the detection and diagnosis of abnormalities via long term surveillance of process signals while the plant is in operation. The term ‘on-line condition monitoring’ of nuclear power plants refers to the following:

— The equipment or system being monitored is in service, active and available (on-line);
— The plant is operating, including operating modes of startups, normal steady state operation and shutdown transients;
— Testing is done in situ, in a non-intrusive, passive way.

The analysis of measured data is not necessarily performed simultaneously with the on-line measurement. Most on-line monitoring (OLM) methods involve off-line and off-site signal processing, modelling, interpretation and decision making.

In the simplest implementation, redundant channels are monitored by comparing each individual channel's indicated measurement to a calculated best estimate of the actual process value; this best estimate of the actual process value is referred to as the process variable estimate. By monitoring each channel's deviation from the process variable estimate, an assessment of each channel's calibration status can be made. An OLM system can also be referred to as a signal validation system or data validation system.

Typically, the conventional calibration of an instrument involves two steps as follows:

— Establishing the calibration status of the instrument. This step is performed by providing the isolated (disconnected from process) instrument with a series of known inputs covering the operating range of the instrument. The output of the instrument is recorded for each input and compared with the acceptance criteria for the instrument.
— Calibration if needed. If the instrument does not meet its acceptance criteria, it is calibrated by providing the same series of input signals as in the previous step, while adjusting the output to meet the acceptance criteria.

The OLM approach requires that data be acquired over a long period of time while the reactor is operating. Unlike in traditional calibration evaluation, the instrument must be in service, on-line (installed and powered up) and providing a signal to its system of application. The entire process of OLM and data collection is passive, non-intrusive and in situ (the instrument is not removed from the process).

The second step of calibration remains the same as in the case of the conventional calibration procedure, although a distinction should be made that the time at which the calibration is scheduled will generally be deferred to an outage period, unless other conditions warrant immediate action.

OLM involves tracking the output of instrument channels over the fuel cycle to identify drift, bias errors, noise and other anomalies. The advantage of this approach is that it identifies calibration problems as they occur, accounts for installation and process condition effects on calibration, and prevents unnecessary calibration of instruments that have maintained their calibrations. Furthermore, it can include most components of an instrument channel in the calibration test as opposed to conventional procedures, which require some components to be isolated and calibrated individually. The method may be used for pressure, level, flow, temperature, neutron flux and other process instrumentation channels, including both safety and non-safety channels in the primary and secondary systems of nuclear power plants.

3.10.2. Options

— Work with national regulators to take credit for OLM in extension of calibration intervals or elimination of calibration in specific applications, based on the establishment of an OLM empirical database, acceptance criteria and procedures complying with national standards approved by the regulator;
— Take no credit for on-line monitoring in place of manual CFTs and calibrations, and only use the OLM information to optimize plant maintenance with all the associated benefits listed.

3.10.3. Associated benefits and challenge

3.10.3.1. Benefits

The OLM methodology can reduce the number of calibrations required during the nuclear power plant's refuelling or maintenance outages, thereby offering the following benefits:

— Reduce the radiation exposure of personnel through elimination of unnecessary calibrations;
— Reduce the possibility of instrument damage during calibration;
— Reduce the time required and the associated costs of instrument channel calibration activities during plant outages;
— Ensure the assessments of the calibration status of instrument channels are continuously available.

Additional benefits from OLM applications that do not directly apply to calibration monitoring of important instrumentation may also be obtained:

— Identification of abnormal plant conditions through monitoring signal interrelationships;
— Condition assessment of plant components and early warning of sensor or component degradation (including sensor calibration drift) or failure;
— Compression of the information from a multitude of instrument channels that may need to be reviewed to only those that are currently being identified by the OLM system as needing attention;
— Faster actions in response to abnormal conditions identified due to the above compression of information;
— Continuous, real time performance monitoring of plant instrument channels, components and systems;
— Validation of signals for other computerized tools.

3.10.3.2. Challenge

Lack of precedent and associated acceptance criteria with regulatory approval in taking credit for OLM in place of fixed calibrations/surveillance for instrument channels.

3.10.4. Precedent decisions / country experience

Sizewell B nuclear power plant in the UK uses a simplified algorithm based on the consistency checking of redundant instrument channels to extend sensor calibration intervals. This technique is not purely 'on-line' in a sense that data acquired on-line are processed off-line to get a conclusion on calibration status, but it is considered by the UK regulator to be sufficient for limited use.

The IAEA has reviewed and reported experience with the use of OLM to improve performance at nuclear power plants. The two publications document Member State experience [58, 59].

3.10.5. Recommendations

OLM techniques provide a passive and non-intrusive means to verify the performance and reliability of nuclear power plant instrumentation channels and other equipment; therefore, it is recommended to utilities to implement OLM techniques. It is also recommended to I&C vendors to consider the advantages of building OLM into the I&C system design of future nuclear power plants.

3.11. ISSUE No. 11: ENVIRONMENTAL QUALIFICATION OF SAFETY SYSTEM PLATFORMS

3.11.1. Introduction

The regulatory positions that are currently being applied in Member States to the qualification of digital equipment for safety systems address the following stressors:

— Environmental;
— Seismic;
— Electromagnetic interference/radiofrequency interference (EMI/RFI).

The IAEA publication Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing [60] describes equipment qualification practices for the benefit of Member States, and addresses basic concepts and processes, establishing, upgrading and preserving equipment qualification, and assessing equipment qualification programmes.

With the introduction of digital equipment, attention to electromagnetic compatibility (EMC) became more common owing to the perception of increased vulnerability to EMI/RFI effects. Newer digital technologies employ faster clock speeds and lower logic voltages, giving rise to concerns about higher emissions levels and increased susceptibility to noise.

As a consequence, the use or integration of new technologies requires particular attention to the equipment's contribution to the electromagnetic environment at the plant, in addition to its susceptibility to EMI/RFI and electrical surges. Consequently, EMC must be considered as part of the qualification of I&C equipment.

A single international standard, IEC 62003 [61], establishes requirements for EMC testing of I&C equipment supplied for use in systems important to safety at nuclear power plants. However, this standard has not been widely adopted to date. NRC Regulatory Guide 1.180 [62] established testing requirements based on specific IEC 61000 [63] series test methods as well as test methods from alternative domestic standards. Other regulators rely on the IEC 61000 series standard or national standards to address EMC aspects of qualification.

Environmental and seismic qualification testing is costly, and the market for nuclear qualified equipment is small. Consequently, environmentally qualified equipment is expensive, and many I&C vendors consider the market too small to warrant the investment that maintaining a nuclear qualified product line requires. Consequently, methods for dedication of commercial grade equipment include guidance on environmental and seismic qualification. Specifically, the Electric Power Research Institute (EPRI) developed guidelines for commercial grade dedication [64] and generic qualification of programmable logic controllers [65], both of which have been endorsed by the NRC and other regulators.

Significant benefit can be seen if the different regulatory authorities use the same criteria for evaluating environmental qualification. The use of different standards sometimes necessitates additional tests to qualify for use in different markets. The main standards used within the industry are IEC 60780 [53] and IEEE 323 [54] for environmental qualification and IEC 60980 [55] and IEEE 344-2004 [56] for seismic testing. These standards start from the same principles and endorse similar methodologies, but differences in detail cause significant problems for the industry because qualification based on one standard is generally not treated as being equivalent to qualification based on the other comparable standard. Consequently, duplicate qualification efforts are often required to satisfy national requirements and specific preferences in various markets.

3.11.2. Options

— Continue the current practice of maintaining multiple sets of qualification requirements (Fig. 2) worldwide for digital equipment used in safety applications including IEC, IEEE and other country specific standards.
— Establish one common set of qualification requirements (Fig. 3) for digital equipment used in safety applications around the world.

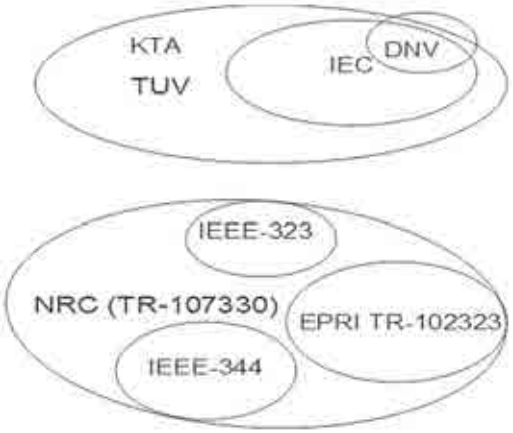


FIG. 2. Multiple sets of qualification requirements. DNV: Det Norske Veritas AS; EPRI: Electric Power Research Institute; IEC: International Electrotechnical Committee; IEEE: Institute of Electrical and Electronic Engineers; KTA: Kerntechnischer Ausschuss; NRC: Nuclear Regulatory Commission; TUV: Technischer Überwachungs-Verein.

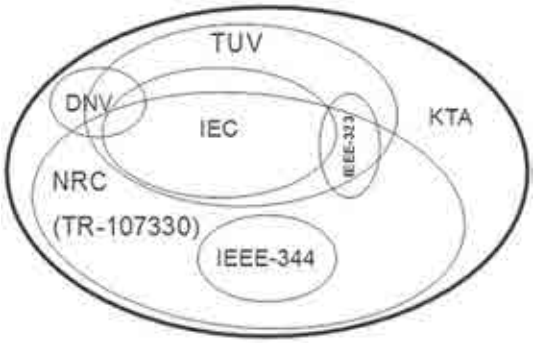


FIG. 3. Common set of qualification requirements. DNV: Det Norske Veritas AS; IEC: International Electrotechnical Committee; IEEE: Institute of Electrical and Electronic Engineers; KTA: Kerntechnischer Ausschuss; NRC: Nuclear Regulatory Commission; TUV: Technischer Überwachungs-Verein.

3.11.3. Associated benefits and challenges

3.11.3.1. Benefits

Gaining multinational acceptance of each of the comparable qualification standards, or harmonizing the standards to achieve a joint logo standard, can eliminate duplicate costs associated with qualification in accordance with multiple standards.

3.11.3.2. Challenges

The first option represents the status quo situation and poses no additional challenges. However, this option leaves unresolved the associated difficulties and unnecessary duplicative costs discussed in the introduction above.

The second option requires either harmonization of standards or development of multinational endorsement of comparable standards. Achieving either condition poses attendant challenges as follows:

— Developing joint logo standards requires agreement among the cognizant standards organizations, establishment of a collaborative process (such as that in place between IEC and IEEE), resolution of technical and formatting differences between standards and acceptance of the harmonized standard by the stakeholder constituency of each organization;
— Gaining multinational acceptance of different qualification standards requires widespread endorsement of comparable standards from different organizations by regulators;
— In either case identified for this option, regulators may establish additional country specific guidance or requirements to tailor the qualification process to address national concerns.

3.11.4. Precedent decisions / country experience

Equipment environmental and seismic qualification globally is well established based on IEEE, IEC or national standards. In the USA, specific additional requirements are imposed on environmental qualification for microprocessor based I&C systems through Regulatory Guide 1.209 [66]. For example, type testing must be performed with representative software installed and functioning while the system is subjected to environmental extremes.

The application of EMI/RFI susceptibility testing is more recent, with IEC and national standards serving as the primary basis in most countries. In the USA, two de facto standard approaches have been developed and applied over the years. Regulatory Guide 1.180 [62] and EPRI TR-102323 [67] both give guidance on appropriate testing practices (e.g. methods and limits) based on IEC 61000 [63] test methods or US Department of Defense military standards.

3.11.5. Recommendation

National and international standards organizations should develop joint logo standards for seismic, environmental and EMI/RFI qualification.

3.12. ISSUE No. 12: IMPACT OF HARDWARE DESCRIPTION LANGUAGE PROGRAMMABLE DEVICES

3.12.1. Introduction

The potential benefits of digital I&C technology include, but are not restricted to, improved accuracy, absence of drift, ease of implementing complex functions, data correlation from multiple distributed sources, high capacity data storage, diagnostics and fault correction, improved human–system interface (HSI), flexibility, and many other capabilities arising from the unique features of digital I&C systems. A successful deployment of digital I&C technology can result in both safety and economic benefits. At the same time, use of computer based digital technology presents challenges, such as CCFs and difficulties with qualification and computer security that require substantial effort for evaluation and safety demonstration as part of the development, commissioning and licensing processes.

As a result, nuclear power plant operators and I&C suppliers may consider other non-computer-based digital technologies, such as devices that may be configured using HDL. These devices may fall into the categories of application specific integrated circuits, complex programmable logic devices (CPLDs) or field programmable gate arrays (FPGAs), commonly referred to as HDL programmable devices (HPDs). Many HPDs are widely used already in other, high integrity safety critical industries, and can offer potential benefits such as 100% testability if appropriate design decisions are made, and may be demonstrably diverse from computer based systems. Despite the attractive features, the use of such programmable devices in safety critical systems for nuclear power plants is relatively new in many countries, and the regulatory approach to licensing such devices may not be clear. Some issues still remain open, such as:

— It is only recently that HPDs (mainly FPGAs) have begun to play an increasing role in the implementation of nuclear power plant I&C functions, therefore the database of reliability numbers, operating experience, lessons learned and good practice is relatively limited compared to computer based digital I&C applications.
— There is currently only one IEC published standard [68] that provides guidance and requirements for HPD based solutions for the nuclear power industry, and to date, this standard has not been widely adopted.
— There are only a few suppliers of HPD based I&C platforms that are qualified for nuclear power plant safety applications with substantial operating experience.
— The methods, languages and design tools for the development of HPD based I&C systems may not be entirely user friendly at present, and so may not yet promote simple and error free implementation of application logic in HPDs.
— HPD design tools may not be as mature as their counterparts in computer based I&C systems, and therefore may be subject to changes that make their suitability for use in safety applications difficult to determine and demonstrate.

3.12.2. Options

— Rely more on HPD based technologies in safety critical applications and gain more experience with increased numbers of applications internationally. The above mentioned disadvantages are not intrinsic to HPD technology; rather, they are the results of not yet having a large enough number of applications, or a consistent approach to qualification. These disadvantages will diminish as HPD based systems gain more acceptance in a variety of nuclear applications.
— Because of lack of wide international consensus on regulations and standards on HPD based technology, and lack of operating experience, HPDs are not widely applied in the nuclear industry, and are used only in non-safety applications, or embedded in smart devices in smaller stand-alone applications. The potentially significant safety benefits of HPDs would not be realized in this case.

3.12.3. Associated benefits and challenges

3.12.3.1. Benefits

As nuclear utilities and regulators become more familiar with the advantages of HPD based technology, HPD systems can provide not only a diverse alternative to the widely used computer based digital I&C systems, but this alternative can become a mature technology on its own for safety and control system applications, playing an increasing role as new I&C designs are expected to meet more stringent diversity and reliability requirements.

3.12.3.2. Challenges

The first option can be successful only if it is part of a coordinated international effort, including harmonizing standards and licensing practices.

For the second option, the challenge would remain of how to make use of the unique advantages of HPD based technology for simple embedded applications.

3.12.4. Precedent decisions / country experience

In the USA, an FPGA based control system was installed in 2009 to replace obsolete equipment in the main steam and feedwater isolation system at the Wolf Creek Generating Station.

In Ukraine, modern FPGA based systems have been installed in safety applications in all operating nuclear power plants, as well as in a research reactor, using the RPC Radiy platform. In the past 10 years, 30 reactor trip systems, 10 reactor power control and limitation systems, 18 ESFASs and 8 nuclear and conventional island control systems have been installed at all four Ukrainian nuclear power plant sites.

In Canada, FPGA technology is being considered for the emulation of obsolete PDP 11 computers used in several non-safety and safety related systems, and utilities are evaluating the replacement of analogue and computer based I&C systems with FPGA based applications. RPC Radiy and Candu Energy have entered into a cooperation agreement for the development of FPGA applications for safety critical functions to be incorporated into their Enhanced CANDU-6 reactor design. The design and manufacture of FPGA based safety related systems to be installed in the Embalse nuclear power plant in Argentina are underway.

In China, China Nuclear Power Engineering Co. is developing FPGA based safety system applications in the new ACP1000 design. The above applications are being considered for the RPS, DAS, ESFAS and post-accident monitoring system. In addition, China Techenergy Co. is developing an FPGA based platform, FitRel, to be used in the design of the DAS for two CPR-1000 units, presently under construction (units 5 and 6 of the Yangjiang nuclear power plant). China's State Nuclear Power Automation System Engineering Company and Lockheed Martin Corporation developed a safety I&C platform, Nuclear Protection and Control (NuPAC), and the NuPAC based RPS to be installed in the China advanced pressurized water reactor CAP-1400. The above two companies are jointly pursuing generic approval from both the NRC and the Chinese nuclear regulator, National Nuclear Safety Administration, for the installation of the NuPAC platform in the CAP series of nuclear power plants. Triconex of Invensys Process Systems is also employing FPGAs for the priority logic modules in the new Fuqing and Fangjiashan nuclear power plants under construction in China.

In the Czech Republic, FPGAs are used in the non-programmable logic (NPL) portion of the Temelin nuclear power plant I&C systems. The NPL is used in priority arbitration between the microprocessor based primary reactor protection system (PRPS) and its diverse protection system (DPS), and the hard wired controls. Other functions of the NPL are to ensure safe failure of the system in the event of a discrepancy between the PRPS and the DPS, as well as the safety diesel load sequencer and associated automatic testing.

In Bulgaria, in units 5 and 6 of the Kozloduy nuclear power plant, RPC Radiy has installed six FPGA based ESFASs.

In Japan, Toshiba has supplied the following FPGA based safety and non-safety systems to operating Japanese nuclear power plants: power range neutron monitoring for boiling water reactors, startup range neutron monitoring for boiling water reactors and radiation monitoring systems for both boiling water reactors and pressurized water reactors. In addition, Toshiba has developed reactor trip and isolation systems for advanced boiling water reactor type plants.

In France, EDF initiated in 2009 the replacement of obsolete electronic control and interface modules in several non-safety systems in their nuclear power plants with FPGA equipment. EDF is currently developing an application based on CPLDs to upgrade the primary pumps rotational speed measurement system. EDF also developed an FPGA based microprocessor emulator to perform a number of I&C functions, including safety critical reactor protection functions in the 1300 MW series of plants.

In the Republic of Korea, FPGAs are used in operating nuclear power plants to perform diagnostic functions in CPLD based system initialization, bus interface, control of input/output signal transfers, memory control and peripheral channel control functions. The Korean nuclear power plants are also planning to use FPGAs in the implementation of component control functions for their engineered safety features.

In Sweden, FPGAs are used in the component interface module (CIM) of the replacement to the unit 2 safety system in the Ringhals nuclear power plant. The CIM acts as the interface between the microprocessor based primary safety actuation system and the actuator, and responds to signals from the independent DAS as well as to operator commands.

3.12.5. Recommendation

Logic implemented on HPDs should be verified according to software V&V standards and guidelines.

3.13. ISSUE No. 13: DIGITAL COMMUNICATIONS

3.13.1. Introduction

It is often desirable to share information between safety related systems and non-safety systems, between systems supporting different lines of defence (e.g. where control and protection functions need information on the same parameter), between different safety classes or between redundancies within safety systems (e.g. where redundant channels vote to make trip decisions). When this is done, precautions are needed to prevent failures from propagating via communication links.

The use of computers in nuclear power plants provides the potential to transfer, via digital communications, a large amount of beneficial information between computers within a single safety channel, between safety channels, between safety classes, and between safety and non-safety systems. Data communication in systems performing safety functions is addressed in IEC 61500 [69]. However, the use of digital communications raises issues such as independence for interchannel communication, contamination of higher safety class systems by lower class systems, and loss of separation between safety and non-safety systems. Improper design of these communications could result in safety systems being unable to perform one or more safety functions, or could initiate spurious actuation of equipment that could challenge other systems.

In computer based systems, a single connection may pass many signals, may involve handshaking between systems and may send data via a communications network rather than point to point connections. This introduces new ways for failures to propagate between connected systems or for failures in the connection itself to cause failure of both connected systems [70]. Consequently, electrical isolation and consideration of functional dependencies are not sufficient to ensure independence when computer to computer communication is involved. The system architecture should aim to avoid adverse effects on safety functions as a result of communication faults or other potential interactions. The system design should also consider the effect of propagating incorrect or incomplete data, potential delays in the propagation of data and measures taken to protect against these issues.

Provisions for interdivisional communication should explicitly preclude the ability to send external software instructions to a safety function processor, unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division.

The nuclear industry has limited experience with the specific means of managing the above mentioned issues. Therefore, the details of communications independence measures are a frequent source of discussion and debate between regulators and developers. Physical, electrical and communication isolation should be ensured where the separation of systems is essential.

Guidance is now provided on the following three key issues:

— Communication between different systems;
— Command prioritization: selection of a particular command to send to an actuator when multiple and conflicting commands exist;
— Control and display stations: use of operator workstations or displays that are associated with multiple safety divisions, system classes and/or with both safety and non-safety functions.

3.13.1.1. Communication between different systems

Communication from lower class systems to higher class systems, and from non-safety to safety equipment should be avoided. However, where this is necessary, a demonstration should be provided showing that there will be no adverse impacts on safety systems, or that potential impacts can be managed and are outweighed by the benefits of providing the information.

3.13.1.2. Command prioritization

Existing diversity and defence in depth guidance indicates that diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse, in order to ensure that the diverse actuation will be unaffected by digital system failures and malfunctions. Accordingly, it should be demonstrated that priority modules using digital logic devices should not be susceptible to CCF.

3.13.1.3. Control and display stations

Operator workstations may be used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. This also applies to workstations that are used to program, modify, monitor or maintain safety systems that are not in the same safety division as the workstation. Multidivisional control and display stations may themselves be safety related or not safety related, and they may include controls and displays for equipment in multiple safety divisions and for equipment that is not safety related, provided they meet the conditions required by their regulatory authority.

It is recommended that where there is communication between safety systems and other systems, the potential negative impacts of those communications should be considered, and measures put in place to manage them. Additional guidance is provided in NRC DI&C-ISG-04 [71].

3.13.2. Options

— Continue to develop country specific standards on acceptable methods of communication between safety channels and also between safety and non-safety components and subsystems.
— Develop a common set of guidelines and requirements that are acceptable to regulators in Member States and that clearly define safety and non-safety communication principles.

3.13.3. Associated benefits and challenge

3.13.3.1. Benefits

Moving forward with the second option will result in a better understanding of common requirements and acceptance criteria and result in fewer unique complex cases requiring additional regulatory focus and resources.

3.13.3.2. Challenge

It is a challenge to gain widescale consensus on a common set of guidelines and requirements on acceptable communication principles.

3.13.4. Precedent decisions / country experience

The NRC SER for the Oconee RPS/ESFAS digital upgrade [10] approved a communication architecture following the general guidance above.

The UK Office for Nuclear Regulation challenged the extensive use of digital communications during the generic design assessment of the UK EPR reactor (the abbreviation has been used to stand for both European Pressurized Reactor and Evolutionary Power Reactor, and the reactor is now known by the abbreviation alone). A report on the outcome of the assessment and describing the regulatory approach is given in GDA Step 4 and Close-out for Control and Instrumentation Assessment of the EDF and AREVA UK EPR Reactor [72].

3.13.5. Recommendations

The safety impact of digital communications and the transfer of information should be considered when making a safety demonstration. Where communications between safety systems and other systems are implemented, it should be demonstrated that there is no adverse impact on safety systems, or that the risks can be managed and are outweighed by the benefits.

3.14. ISSUE No. 14: SAFETY CLASSIFICATION AND FUNCTION OF A SOFT CONTROLLER

3.14.1. Introduction

Digital I&C systems are mostly designed using digital technologies to process data efficiently in a compact and efficient manner, where a huge number of manual switches dedicated spatially are replaced with soft controls implemented by software.

Diverse manual switches/controls for system level and minimum inventory switches are provided in a safety console against the CCF of digital plant protection systems and diverse ESFASs. Manual control switches on the safety console are designed for the purpose of controlling safety related systems during and following design basis events using hardwire based control.

In accordance with the requirements of IEEE Standard 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Sections 6.2 and 7.2 [37], the soft controls shall be designed as safety components because they are used to perform the safety functions and corresponding protective actions for each design basis event. However, if the safety function can also be completed (backed up) using the manual controls on the safety console, such as manual ESFAS switches and minimum inventory switches, the soft controls may be classified as non-safety, as long as the priority applies to the safety controls, and safety and non-safety are adequately isolated.

Soft controls are used in controlling both safety systems and non-safety systems. Therefore, the existing regulations, regulatory guidelines and industrial standards require that equipment and circuits used in both safety and non-safety systems should be classified into safety classes and designed in such a manner that they meet the requirements comparable with the safety system.

Manual control via the soft control feature of the computer based system may cause issues related to HSI requirements and to soft control performance. In this case, the performance of soft controls should be verified through dynamic simulation to make sure that operator actions can be taken in a timely manner under all anticipated situations.

The control of the components of conventional ESFASs is implemented by the dedicated controls using the individual hand switches designed as safety components with the physical separation between channels. The desired independence between channels is maintained, from the perspective of signal transmission, even though they are not separated physically.

3.14.2. Option

This significant design change makes it more difficult to ensure independence between safety and non-safety signals and to perform software V&V.

In accordance with the requirements of codes and standards, manual switches used to control the safety related components are classified as safety components. Therefore, the regulatory position is that the soft control that is functionally equivalent to manual switches should also be classified as safety components. This means, for instance, that the electrical isolation and physical separation between channels should be maintained.

3.14.3. Associated benefits and challenges

3.14.3.1. Benefits

In the design of the main control room or the remote shutdown panel, existing manual switches are replaced with soft controls on the flat panel display. The manual switches replaced with a soft controller can reduce the cost and optimize the operational aspects.

3.14.3.2. Challenges

The safety classification of soft controls should be considered carefully because they directly control the components related to the safety systems during and following the design basis events. When addressing soft controls, a methodology must be put into place that adequately addresses separation of safety and non-safety controls, and which does not challenge diversity and defence in depth principles. To meet the manual control requirements, a method to address the priority of safety signals must be implemented. Dedicated safety controls (e.g. a safety qualified video display unit or a qualified manual control) may be provided as referenced in IEEE 7-4.3.2-2003, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations [8], Section 5.16.3, Diverse Manual Controls and Displays.

3.14.4. Precedent decisions / country experience

For the Korean Shin-Kori units 3 and 4, KINS has approved a dedicated safety soft controller for the safety system and a separate soft control for the non-safety system.

3.14.5. Recommendations

— Soft controller functions should meet the communication independence criteria between safety and non-safety components, and should give priority to safety actuation commands. Hazard and safety analyses should also be conducted.
— Diversity and defence in depth principles should not be challenged by the potential for software CCF to affect both manual controls and other layers of protection.
— Soft controls should be classified as safety components.

3.15. ISSUE No. 15: FORMAL METHODS OF SOFTWARE DEVELOPMENT

3.15.1. Introduction

‘Formal methods’ refers to the use of mathematics and logic as a framework for specifying, defining and verifying systems (software and/or hardware). These methods may provide the basis for the precise definition of consistency, completeness and correctness of requirements, designs and tests. Formal methods have been promoted as a means of increasing the reliability of safety critical systems, but the industrial acceptance of such methods has been slow. This appears to be due to difficulties in understanding and training in the underlying mathematical nature of these methods, and the lack of widely available tool support.

Part 3 of the IEC 61508 [3] standard highly recommends formal methods to be used at safety integrity level (SIL) 4 and could be viewed as applicable to class 1 systems performing functions such as reactor protection.

However, mathematical analysis has important constraints so that it can only be used in limited cases, as current theory cannot easily combine all the features and properties found in a real system.

In practice, formal methods support establishing precise specifications so that these descriptions enable analysis, verification and proof.

IEC 60880 [50] noted that tools for formal specification and design methods can be classified as constructive or analytical. Constructive tools are used to support the specification, design and code phases of development, and may include a mathematical text or graphical editor, automatic code generation and automatic generation of the proof obligations arising during the design steps based on logical reasoning. Analytical tools enable checking of the specification, design and code, and may include a syntax checker, a semantic checker, a formal proof generator, an animator and a compliance analyser.

The European regulators [15] identified their common position regarding formal methods as giving no credit in a safety demonstration for the use of a formal method without due consideration of the specific evidence provided by its use. They also identified that the formal descriptions and mathematical analysis methods need to be carefully selected with respect to their intended application, that they should be understandable by all technical staff involved and that a syntactical verification of the formal descriptions should be performed. The regulators emphasized that adequate tools and training should be provided, and that methods based on application oriented graphical languages connecting components in the logic diagrams should be verified to satisfy syntactic and semantic rules, and that simulation and/or animation tools should be incorporated.

3.15.2. Options

— Select and justify carefully the formal descriptions and mathematical analysis methods with respect to their intended applications.
— Continue with current practices.

3.15.3. Associated benefits and challenges

3.15.3.1. Benefits

— Formal methods can be used to systematize completeness and consistency verification of system specifications, and demonstrate syntactic correctness of software specifications.
— Using mathematical analysis for verification of a piece of code demonstrates that it is a complete and correct translation of its specification.
— Proof techniques can be used to validate that an unsafe state is not reachable.

3.15.3.2. Challenges

— In practice, use of mathematical formal analysis is problematic, as a single analysis can cover only specific aspects, because there is no uniform theory that can combine all the features of software.
— The availability of software engineers who are knowledgeable and experienced in the use of formal methods is currently limited.

3.15.4. Precedent decisions / country experience

NRC NUREG-0800, Appendix 7.0-A, [30] encourages the use of formal or semiformal methods during software development V&V, but notes that formal methods do not yet represent a complete solution to producing high quality software.

In Canada, the Darlington shutdown system design is an example where formal methods have been used with some success. IAEA-TECDOC-1328 [73] identifies that Darlington nuclear power plant's effort was extremely expensive, but this was at least partially a result of imposition of the formal method after the code was finished. The conclusion based on this early experience was that there was not convincing evidence that the resulting increase in safety was worth the cost. However, there have been significant further efforts since that time.

Analysis tools based on the Lustre formal language have been widely used in the nuclear industry by companies in various countries (e.g. China, France and the Republic of Korea), and many current operating reactors use some digital I&C systems that were developed successfully using these tools.

3.15.5. Recommendations

— Use of formal methods should be encouraged to improve quality of software requirements, design and V&V.
— Effective tool support is critical, and using tools based upon graphical approaches promotes understanding and usage.
— Formal methods are not generally available to support all elements of the software life cycle. Therefore, when formal methods are used, care must still be taken to ensure that issues are not overlooked simply because they cannot be described by the formal method.

3.16. ISSUE No. 16: USE OF WIRELESS TECHNOLOGY

3.16.1. Introduction

The reduced cost of Ethernet based networks is driving fast changes in the technology of equipment used in industrial applications. A side effect of this is the proliferation of wireless technology and Wi-Fi wireless protocols that are essentially wireless Ethernet. It is possible for devices to communicate via Wi-Fi at data rates up to 600 Mbps as if they were connected by cable.

The availability of additional data provided by enhanced communications is often beneficial. However, the use of wireless technology in digital communications causes problems in security that have not been previously considered.

Wireless technology provides a solution where the high cost of industrial wiring is problematic and also provides an ultimate barrier to electrical surges introduced in field equipment through field wiring. The potential cost reductions arising from the avoidance of wire/cable installation and maintenance is creating an expanding market for wireless devices. System architects continually find new applications for industrial measurements and controls that make use of wireless devices.

However, any wireless technology can be challenged by the electrically noisy environment of a process plant or a factory floor where there are many sources of EMI such as large motors, motor controllers, electrical devices, process controllers, digital equipment and radio communications equipment. Most of the physical structures in a nuclear power plant are constructed of thick reinforced concrete, and large steel components such as tanks, enclosures, containment, piping, valves, motors, pumps and ventilation systems. These SSCs result in highly reverberant radiofrequency environments that can cause multipath interference in wireless signals. In addition, the wireless devices themselves are potential sources of EMI.

A number of relatively new wireless network protocols promise to make these problems manageable:

— WirelessHART: A de facto standard based upon the IEEE 802.15.4-2011 standard [74] modified to hop among the 15 or 16 channels in the 2.4 GHz industrial, scientific and medical (ISM) band supported by the HART Communication Foundation; it is an IEC publicly available specification. Field devices belong to a mesh network with a secure method of building and repairing the mesh. WirelessHART devices may also be set to transmit data using a publishing method. An IEC working group is developing an international standard for WirelessHART. There are probably more than 25 million WirelessHART instruments in service.
— ISA100.11a: This protocol also uses the same IEEE 802.15.4-2011 standard [74] with channel hopping in the ISM band similar to WirelessHART. ISA100.11a protocols provide secure end-to-end message delivery and confirmation. Unlike WirelessHART, each network segment may use a different hopping pattern and its own allocated time slot, which allows large networks to form where segments may overlap. ISA100.11a also uses mesh networking, but does not allow devices at the edge of the network to route messages to other devices. This can increase security by preventing unauthorized devices to access plant networks from outside the plant. The ISA and ANSI standard [75] defines the ISA100.11a protocol, but it has not yet been endorsed by the IEC.

— IEEE 802-11n: The feature of Wi-Fi-n that is most appealing to industrial use is its adoption of multiple input, multiple output (MIMO) technology. MIMO technology has the demonstrated potential to eliminate the adverse effects of reflections. Using MIMO technology achieves improved reception by detecting the multipath signals and either eliminating them or phase shifting them to amplify the received signal. Early experiments suggest using Wi-Fi-n can achieve excellent behaviour in both process plants and factories that are notorious for their 'canyons of steel', the cause of poor performance of earlier Wi-Fi protocols. Recently, the IEEE have issued the IEEE 802-11n-2012 standard [76].

Wireless devices can often be designed for low power consumption. Such devices can be powered by batteries that do not need frequent replacement. Energy harvesting from natural sources is also starting to be used to extend the life of device batteries or to directly power the wireless device. With such methods, wireless devices can avoid the need for power supply cables as well as communications cables.

3.16.1.1. Usage at nuclear power plants

In existing nuclear power plants, it is often impractical, or cost prohibitive, to add new sensors if they must be hardwired to a monitoring location. This strongly discourages installation of additional condition monitoring. Wireless sensors may help to resolve this issue. Use of wireless technology to extend plant communication networks has shown promise in the US nuclear industry, resulting in improved dissemination of information and overall personnel efficiency. Worldwide, nuclear power plants have taken advantage of wireless technologies in a number of ways that include:

— Voice over Internet protocol phones for voice communications throughout the plant.
— Supporting the use of laptops or personal digital assistants for the upload of data to the plant network, general network access and data communications.
— Condition monitoring, such as wireless vibration sensors for traditional condition monitoring of rotating equipment, and facilities monitoring. This is seen as one of the most beneficial uses of wireless technology in the nuclear power industry.
— Supporting in-service inspections (such as containment integrated leak rate tests) that use many temporarily installed sensors for gathering data.
— Wireless cameras for physical security purposes, analogue gauge readings or personnel monitoring. This has proven to be a simple and effective use of the technology. Specifically, it is obviously helpful to reduce operator workload for the periodic recording of any local panel indication.
— Wireless personnel dosimetry.
— Wireless controls for crane operation.
— System performance monitoring.

As experience and confidence is gained, wireless technology applications may be extended from ancillary functions to monitoring of plant conditions for operator information and control. For example, wireless communication might eventually be used in safety related functions such as core cooling monitoring and post-accident monitoring. Such wireless monitoring may offer advantages by providing measurements that are diverse from those of current wired sensing loops.

Use of wireless technology creates the challenge of maintaining security and privacy to communication networks. Encryption standards and network architectural design can provide for secure and reliable transmission of data. Such approaches are accepted in other industries for the communication of highly sensitive information.

3.16.2. Option

Actively pursue the deployment of wireless technology in monitoring and diagnostics applications in nuclear power plants in order to gain experience and develop knowledge that will allow future use of wireless in more demanding plant applications.

3.16.3. Associated benefits and challenge

3.16.3.1. Benefits

The potential benefits of using wireless technology should be considered. The following aspects are important:

— Potential for decreased plant personnel exposure to radiation;
— Reduced costs of new system installations;
— Reduced maintenance costs;
— Increased availability of information.

3.16.3.2. Challenge

The current challenge relates to the building of trust that wireless technology can deliver the benefits projected and that the difficulties can be adequately managed. The regulatory position is, in many cases, not clear, and the resulting uncertainty leads to designers being reluctant to consider wireless technologies.

3.16.4. Precedent decisions / country experience

The South Texas and Comanche Peak nuclear power plants in the USA have implemented extensive projects with wireless technology. These were in non-safety applications, but the experience gained will be useful to support broader applications of wireless technology in the future.

Entergy Nuclear adopted wireless technology at its River Bend Nuclear Station in the USA by applying wireless pressure transmitters on the high pressure turbine to monitor its performance as a baseline for comparison to a new turbine that will be installed in the future. This saved US $4 million.

Licensees in the UK have successfully implemented systems that use wireless technologies to transmit reactor parameters outside nuclear power plant buildings in beyond design basis accidents.

3.16.5. Recommendations

— Nuclear power plant operators should consider the staged implementation of wireless technology for a variety of I&C tasks, including operations, to gain experience and confidence.
— Appropriate measures should be applied to resolve security issues with wireless technology.
— Protective measures should be applied to ensure delivery and integrity of signal transmission.

3.17. ISSUE No. 17: RELIABILITY (TAKING CREDIT FOR DIGITAL SYSTEMS IN PROBABILISTIC RISK ASSESSMENT)

3.17.1. Introduction

The primary licensing challenge in the area of reliability is to provide clear guidance on how digital I&C systems can be included within PRAs. Digital systems present difficulties for traditional methods owing to their use of software for which systematic failure modes dominate the random modes of failure normally modelled in PRAs. This introduces the potential for complex interdependencies as I&C systems influence most aspects of plant control, protection and monitoring. Hence, the inclusion of I&C CCF in PRAs is very important, as sensitivity analysis becomes more important to fully understand the level of risk associated with operating reactors with new digital systems.

In most cases, the deterministic approach recommended in international standards is to be used for safety demonstration of systems. However, the use of PRAs may lead to the need for reliability targets to be set for I&C systems, including the software in some countries. The issue discussed here concerns only those cases in which reliability targets are set for software, and the justification is to be based on quantitative reliability.

Very high reliability figures cannot be formally justified for a piece of software. Failure probabilities lower than 10^{-4} are rarely claimed or justified, even in a highly diversified software system. For example, IEC 61226 [35] states that:

> "For an individual system which is specified and designed in accordance with the highest quality criteria, a figure of the order of 10^{-4} failure/demand may be an appropriate overall limit to place on the reliability that may be claimed, when all of the potential sources of failure due to the specification, design, manufacture, installation, operating environment, and maintenance practices, are taken into account. This figure includes the risk of CCF in the redundant channels of the system, and applies to the whole of the system, from sensors through processing to the outputs to the actuated equipment. Claims for better reliabilities than this are not precluded, but will need special justification ..."

It is generally agreed that there is no current technical basis for developing quantitative software reliability values and associated regulator defined acceptance criteria. However, the use of software statistical testing (SST) techniques offers the possibility of a quantitative demonstration [15].

Currently, there are experiences with nuclear related and software based systems that provide for employing empirical reliability data more effectively than before. In addition, advances in computing capabilities mean that SST is becoming more practicable as a form of evidence. This evidence could have an important role in the assurance of nuclear I&C systems.

In addition, software reliability should take into consideration all the information obtained by design (e.g. diversity) and V&V. This approach can be based on the identification of failure modes of interest, of the failure mechanisms that could lead to these modes and on the effectiveness of the measures taken to prevent given mechanisms. It will also consider the implication of levels of defence and diversity and implementation technologies.

There is a future for risk informed decision making; operational experience feedback will provide plant specific data to the PRA model. The common position of the European regulators [15] is that:

— Low reliability claims for a single software based system (on demand or dangerous failures per year) should be treated with extreme caution.
— The safety plan should identify how achievement of the reliability targets will be demonstrated.
— The sensitivity of the plant risk to variation of the reliability targets should be assessed.
— Software of the highest possible quality should be used, and claims of high reliability involving multiple low reliability computer based systems should not be allowed.
— The reliability from each executable software component (operating system, application software, sensing and actuation devices, communication protocols, etc.) should be considered.

3.17.2. Options

— Continue with only a deterministic process of regulatory reviews, and not taking credit for risk insights and/or PRA results to support decisions regarding digital I&C system architectures.
— Complete and validate the R&D necessary to implement an effective and efficient methodology for inserting risk insights into the regulatory programme approval processes for digital systems and equipment.

3.17.3. Associated benefits and challenges

3.17.3.1. Benefits

— Licensing interactions can benefit from using risk insights to inform decisions and to streamline the licensing processes for digital systems.
— The use of SST provides the potential to derive an estimate of demonstrated system reliability.

3.17.3.2. Challenges

Owing to data limitations and the lack of consensus in the technical community on appropriate modelling tools, the assessment of digital I&C system risk for nuclear plant systems in a number of countries has been limited to examining assumptions, performing sensitivity studies and evaluating importance measure values. The resulting plant risk then is assessed against the regulatory defined safety goals.

While a variety of methods might be acceptable for some applications, regulators are not yet confident in how specific decisions should be mapped to levels of PRA detail. While bounding PRA analyses may provide the insights needed in very specific cases, the regulators in these countries have made it clear that they believe that realistic risk assessments should be performed whenever possible, because bounding analyses may mask important safety insights and can distort a plant's risk profile, and bounding analysis may not adequately address unique digital system failure modes. Regulatory reviewers should be aware that bounding risk analyses may alter or mask safety insights in areas such as importance measure values and sequences identified as dominant, and may not be capable of modelling or bounding unique digital failure modes.

Software is tailored to specific requirements, and thus, it is functionally and structurally different from any other software. Accordingly, if a technically sound method or process was employed to obtain a probabilistic parameter, such as its probability of failure, of a software application, then in general, this probability cannot be applied to any other software. Therefore, substantial technical justification must be given for assuming that a probabilistic parameter from one set of software can be used for different software.

3.17.4. Precedent decisions / country experience

In the UK, most stations have safety cases based on PRA techniques. Sizewell B was the first to embed the PRA into a 'Living Safety Case' and limited the claim made on the PPS to 10^{-4}. Similarly, the UK generic design assessment of the UK EPR [77] observed that the original failure probabilities used in the PRA, of 10^{-5} for the RPS/ESFAS and 10^{-4} for the normal control system, were either beyond or at the normal limits for computer based safety systems, and so the claims were subsequently reduced to 10^{-4} and 10^{-2}, respectively. The UK regulator highlights a distinction between dependability and dependence. The dependability of a system is the degree to which it could be relied upon, whereas dependence on a system is the degree to which it is relied upon. These only become the same in the unusual circumstance that the true reliability of the system is known; otherwise, the difference between them is the safety margin to allow for the uncertainty. The more uncertain the reliability of the particular system in question, the greater the safety margin that is required. Such uncertainties abound where advanced systems are used; the greater the complexity and sophistication, the greater the uncertainty in reliability [9].

An example of digital I&C systems being included within the PRA is provided by the EPR. The approach taken uses the Compact Failure Model which is a simplified functional representation of the I&C systems. Basic events are included in the PRA for the sensor, logic solving and actuation parts of each I&C system function. The failure probability for the common logic part takes into account the potential for CCF that may be introduced by the use of common technology and software [78].

The NRC has published interim staff guidance [79] in this area, and recognizes that if the same digital I&C hardware is used for implementing several I&C systems that perform different functions, a failure in the hardware, software or system of the I&C platform may adversely affect all these functions at the same time. Consequently, it requires that this impact should be explicitly included in the probabilistic model and that the probabilistic model of the digital I&C system should be fully integrated with the probabilistic model of other systems. The guidance also requires that in addition to considering failure to operate on demand, the PRA must also ensure that spurious actuations of diverse backup systems or functions are evaluated and the overall risk impact documented. The NRC also observes that the data for hardware failure rates (including CCF) will likely be more robust than the software failure data, and so if the applicant claims extremely low CCF rates (especially for software), a NRC audit of data calculations may be warranted.

In Finland, the software is tested by supplying it with input values. As exhaustive testing is not manageable, the tester is faced with the problem of selecting a subset of the input domain that is well suited for revealing the (unknown) faults. The usual method for generating test inputs proceeds according to the deterministic principle. This includes the selection of an a priori set of test inputs such that each element is tried at least once. However,

a major limitation is due to the imperfect connection of the criteria with the real faults: testing only once, or a few times, each element defined by such imperfect criteria is not enough to ensure a high fault exposure power.

To overcome a deficiency in SST, test cases are sampled randomly according to a probability distribution over the input space. Such a distribution represents the operation of the software under the conditions in which it is required to function. In many countries, as stated above, the use of risk insights in evaluating digital systems has been very limited.

3.17.5. Recommendations

— For many countries, the recommended course would be to continue the deterministic only process of regulatory reviews, not taking credit for quantitative software reliability until research discussed in the next recommendation has been proven.
— Complete and validate R&D necessary to implement an effective and efficient methodology for inserting risk insights into the regulatory programme approval processes for digital systems and equipment.
— SST is still considered a useful technique because it explores for design faults in a way that is different to other testing methods.

4. SUMMARY

I&C systems provide an essential role in controlling and providing feedback on the status of nuclear power plants, and protecting them from unwanted events. I&C technology continues to develop in ways that have the potential to further improve control and protection of nuclear power plants, but which can also potentially compromise the safety of these plants. This publication records the technical challenges posed by I&C systems to nuclear power plant operators, developers, suppliers and regulators, with the intention that the industry can better understand and benefit from shared experience, recent technology developments and emerging best practices. The publication discusses the technical challenges of designing, developing, implementing, licensing and maintaining digital I&C systems, rather than examining the various vendor specific product lines, plant specific architectures and country specific licensing frameworks and processes. Examples of experience in applying new and novel I&C approaches are given with the intention of highlighting successes and stimulating debate, not to promote any named product.

The primary objectives of this publication have been to:

— Highlight the technical challenges posed by I&C systems and some of the more frequently encountered major issues. It was not the intention to present an exhaustive list of issues, and it is recognized that other issues exist and that more may emerge in the future.
— List credible available options, and define the benefits and challenges of each.
— Identify existing precedents for resolving problems.
— Where possible, suggest technical solutions to common challenges and to the development of a unified regulatory framework for consistent licensing.

The final objective is to encourage the industry to move towards effective resolution of the challenges posed by I&C systems and a more common position on these technical issues, thereby providing the industry with the confidence to move forward with improved designs for existing and for new plants.

Finally, the information provided in this publication is intended to serve as a resource that also enables new technical participants and newly engaged countries to become aware of the scope, range of technologies, and key benefits and challenges arising from the application of I&C systems within nuclear power plants. The transfer of this knowledge should facilitate the safe implementation of nuclear power and support the transition within the nuclear industry to modern digital I&C systems.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna (2007).

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Rep. IEC 61508, IEC, Geneva (2010).

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — General Requirements for Systems, Rep. IEC 61513, IEC, Geneva (2003).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety — Safety Instrumented Systems for the Process Industry Sector, Rep. IEC 61511, IEC, Geneva (2003).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants, IAEA-TECDOC-1327, IAEA, Vienna (2002).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety – Surveillance Testing, Rep. IEC 60671, IEC, Geneva (2007).

[8] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Standard 7-4.3.2-2003, IEEE, New York (2003).

[9] HEALTH AND SAFETY EXECUTIVE, OFFICE FOR NUCLEAR REGULATION, Technical Assessment Guide — Safety Systems, T/AST/003 Issue 6, ONR, Bootle (2011).

[10] NUCLEAR REGULATORY COMMISSION, Oconee Nuclear Station, Units 1, 2 and 3, Issuance of Amendments Regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protective System (RPS/ESPS) Digital Upgrade, Safety Evaluation Report TAC Nos. MD7999, MD8000 and MD8001, US NRC, Washington, DC (2010).

[11] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Software Verification and Validation, IEEE Standard 1012, IEEE, New York (1998).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, IAEA Technical Reports Series No. 384, IAEA, Vienna (1999).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Software Important to Safety, Technical Reports Series No. 397, IAEA, Vienna (2000).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[15] HEALTH AND SAFETY EXECUTIVE, OFFICE FOR NUCLEAR REGULATION, Licensing of Safety Critical Software for Nuclear Reactors. Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations (2013),
http://www.hse.gov.uk/nuclear/software.pdf

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Specification of Requirements for Upgrades Using Digital Instrument and Control Systems, IAEA-TECDOC-1066, IAEA, Vienna (1999).

[17] HEALTH AND SAFETY EXECUTIVE, Out of Control — Why Control Systems go Wrong and how to Prevent Failure, 2nd edn, HSE Books, London (2003).

[18] THE STANDISH GROUP, Chaos, The Standish Group Report (1995),
http://www.projectsmart.co.uk/docs/chaos-report.pdf

[19] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Guide to Developing System Requirements Specifications, IEEE Standard 1233, IEEE, New York (1998).

[20] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for Software Requirements Specifications, IEEE Standard 830, IEEE, New York (1998).

[21] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Quality Management Systems — Guidelines for Configuration Management, ISO Standard 10007, ISO, Geneva (2003).

[22] AMERICAN NATIONAL STANDARDS INSTITUTE / ELECTRONIC INDUSTRIES ALLIANCE, National Consensus Standard for Configuration Management, ANSI/EIA-649-A, ANSI/EIA, New York (2004).

[23] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Software Configuration Management Plans, IEEE Standard 828, IEEE, New York (2005).

[24] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Software Test Documentation, IEEE Standard 829, IEEE, New York (2009).

[25] UNITED STATES DEPARTMENT OF DEFENSE, Defense Handbook: Configuration Management Guidance, MIL-HDBK-61A, DoD, Washington, DC (2001).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Configuration Management in Nuclear Power Plants, IAEA-TECDOC-1335, IAEA, Vienna (2003).

[27] NUCLEAR REGULATORY COMMISSION, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.169, US NRC, Washington, DC (1997).
[28] NUCLEAR REGULATORY COMMISSION, Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, Rep. NUREG/CR-6303, US NRC, Washington, DC (1994).
[29] NUCLEAR REGULATORY COMMISSION, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs, Policy Issue SECY-93-087, US NRC, Washington, DC (1993).
[30] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for Light Water Reactors: Chapter 7, Instrumentation and Control, Rep. NUREG-0800, BTP 7-19, US NRC, Washington, DC (2003).
[31] NUCLEAR REGULATORY COMMISSION, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, Rep. NUREG/CR-7007, US NRC, Washington, DC (2010).
[32] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Requirements for Coping with Common Cause Failure (CCF), Rep. IEC 62340, IEC, Geneva (2007).
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-1.5, IAEA, Vienna (2009).
[34] EUROPEAN UTILITY REQUIREMENTS ORGANIZATION, European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 10: Instrumentation and Control and Man-Machine Interface, EUR (2001).
[35] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Classification of Instrumentation and Control Functions, Rep. IEC 61226, 3rd edn, IEC, Geneva (2009).
[36] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).
[37] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Standard 603, IEEE, New York (1998).
[38] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).
[39] AMERICAN NUCLEAR SOCIETY, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants, ANS Standard N-18.2, ANS, La Grange Park, IL (1983).
[40] NUCLEAR REGULATORY COMMISSION, Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance, Regulatory Guide 1.201, US NRC, Washington, DC (2006).
[41] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).
[42] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Security Management Systems, ISO/IEC Standard 27000 Series, ISO/IEC, Geneva (2013).
[43] NUCLEAR REGULATORY COMMISSION, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, US NRC, Washington, DC (2010).
[44] NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, Rep. NEI 08-09, Rev. 6, NEI, Washington, DC (2010).
[45] NUCLEAR REGULATORY COMMISSION, Protection of Digital Computer and Communication Systems and Networks, 10 CFR 73.54, US NRC, Washington, DC (2009).
[46] NUCLEAR REGULATORY COMMISSION, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.152, Rev. 3, US NRC, Washington, DC (2011).
[47] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).
[48] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Requirements for Security Programmes for Computer-Based Systems, Rep. IEC 62645, IEC, Geneva (2013).
[49] NUCLEAR REGULATORY COMMISSION, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.152, Rev. 2, US NRC, Washington, DC (2006).
[50] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer Based Systems Performing Category A Functions, Rep. IEC 60880, IEC, Geneva (2006).
[51] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer Based Systems Performing Category B or C Functions, Rep. IEC 62138, IEC, Geneva (2004).
[52] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Developing Software Life Cycle Processes, IEEE Standard 1074-2006, IEEE, New York (2006).
[53] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Electrical Equipment of the Safety System — Qualification, Rep. IEC 60780, 2nd edn, IEC, Geneva (1998).

[54] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE Standard 323, IEEE, New York (2003).
[55] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Recommended Practices for Seismic Qualification of Electrical Equipment of the Safety System for Nuclear Generating Stations, Rep. IEC 60980, IEC, Geneva (1989).
[56] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE Standard 344-2004, IEEE, New York (2004).
[57] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Standard 338-2000, IEEE, New York (2000).
[58] INTERNATIONAL ATOMIC ENERGY AGENCY, On-line Monitoring for Improving Performance of Nuclear Power Plants, Part 1: Instrument Channel Monitoring, IAEA Nuclear Energy Series No. NP-T-1.1, IAEA, Vienna (2008).
[59] INTERNATIONAL ATOMIC ENERGY AGENCY, On-line Monitoring for Improving Performance of Nuclear Power Plants, Part 2: Process and Component Condition Monitoring and Diagnostics, IAEA Nuclear Energy Series No. NP-T-1.2, IAEA, Vienna (2008).
[60] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Report Series No. 3, IAEA, Vienna (1998).
[61] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Requirements for Electromagnetic Compatibility Testing, Rep. IEC 62003, IEC, Geneva (2003).
[62] NUCLEAR REGULATORY COMMISSION, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Regulatory Guide 1.180, US NRC, Washington, DC (2003).
[63] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electromagnetic Compatibility (EMC), Testing and Measurement Techniques, Overview of Immunity Tests (IEC 61000-4 series), Rep. IEC 61000-4-1, IEC, Geneva (2007).
[64] ELECTRIC POWER RESEARCH INSTITUTE, Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications, Rep. EPRI TR-106439, EPRI, Palo Alto, CA (1996).
[65] ELECTRIC POWER RESEARCH INSTITUTE, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plans, Rep. EPRI TR-107330, EPRI, Palo Alto, CA (1996).
[66] NUCLEAR REGULATORY COMMISSION, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, Regulatory Guide 1.209, US NRC, Washington, DC (2006).
[67] ELECTRIC POWER RESEARCH INSTITUTE, Guidelines for Electromagnetic Interference Testing in Power Plants, Rep. EPRI TR-102323, EPRI, Palo Alto, CA (1994).
[68] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions, Rep. IEC 62566, IEC, Geneva (2012).
[69] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Data Communication in Systems Performing Category A Functions, Rep. IEC 61500, IEC, Geneva (2009).
[70] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Industrial Communication Networks — Profiles — Part 3: Functional Safety Fieldbuses — General Rules and Profile Definitions, Rep. IEC 61784-3, IEC, Geneva (2008).
[71] NUCLEAR REGULATORY COMMISSION, Highly-Integrated Control Rooms — Communications Issues (HICRc), Interim Staff Guidance DI&C-ISG-04 Rev. 1, US NRC, Washington, DC (2009).
[72] HEALTH AND SAFETY EXECUTIVE, OFFICE FOR NUCLEAR REGULATION, GDA Step 4 and Close-out for Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor, Assessment Rep. ONR-GDA-AR-11-022, Rev. 1, ONR, Bootle (2013).
[73] INTERNATIONAL ATOMIC ENERGY AGENCY, Solutions for Cost Effective Assessment of Software Based Instrumentation and Control Systems in Nuclear Power Plants, IAEA-TECDOC-1328, IAEA, Vienna (2002).
[74] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Information Technology — Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Standard 802.15.4-2011, IEEE, New York (2011).
[75] INTERNATIONAL SOCIETY OF AUTOMATION, Wireless Systems for Industrial Automation: Process Control and Related Applications, Rep. ISA-100.11a, ISA, Research Triangle Park, NC (2011).
[76] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Information Technology — Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11n-2012, IEEE, New York (2012).
[77] HEALTH AND SAFETY EXECUTIVE, Step 3 Control and Instrumentation Assessment of the EDF and AREVA UK EPR, Assessment Rep. AR 09/038-P, HSE Nuclear Directorate, Bootle (2009).
[78] ÉLECTRICITÉ DE FRANCE / AREVA NP, UK EPR, PCSR Sub-chapter 15.1 — Level 1 PSA, Rep. UKEPR-0002-151, Issue 05, EDF/AREVA (2012),
http://www.epr-reactor.co.uk/ssmod/liblocal/docs/PCSR/Chapter%2015%20-%20Probabilistic%20Safety%20Analysis/Sub-Chapter%2015.1%20-%20Level%201%20PSA.pdf

[79] NUCLEAR REGULATORY COMMISSION, Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments, Interim Staff Guidance ISG-03, US NRC, Washington, DC (2008).

GLOSSARY

This Glossary provides definitions for a wide range of terms used in the nuclear instrumentation and control area. The origin of the definition is the IAEA Safety Glossary[1] unless otherwise indicated by a footnote.

accident. Any unintended event, including operating errors, equipment failures and other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

accident conditions. Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents. Examples of such deviations include a major fuel failure or a loss of coolant accident.

anticipated transient without scram. For a nuclear reactor, an accident for which the initiating event is an anticipated operational occurrence and in which the fast shutdown system of the reactor fails to function.

availability. The fraction of time for which a system is capable of fulfilling its intended purpose. Reliability represents essentially the same information, but in a different form.

beyond design basis accident. Accident conditions more severe than a design basis accident.

calibration. A measurement of, or adjustment to, an instrument, component or system to ensure that its accuracy or response is acceptable.

channel. An arrangement of interconnected components within a system that initiates a single output. A channel loses its identity where single output signals are combined with signals from other channels (e.g. from a monitoring channel or a safety actuation channel).

channel check. Process by which a plant operator compares the reading of redundant instrument channels on a regular basis to verify that these are in good agreement according to a predefined criteria.[2]

common cause failure. Failure of two or more structures, systems and components due to a single specific event or cause. For example, a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a human induced event, saturation of signals, or an unintended cascading effect from any other operation or failure within the plant or from a change in ambient conditions.

computer (digital). A programmable functional unit, which consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs and that can perform substantial computation including arithmetic and logic operations without human intervention during a run. A digital computer is any device that includes digital computer hardware, software (including firmware) and interfaces.[3]

---

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna (2007).

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electropedia: The World's Online Electrotechnical Vocabulary, IEV Ref. 395-07-114 (2014), http://www.electropedia.org/.

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer Based Systems Performing Category A Functions, Rep. IEC 60880, IEC, Geneva (2006).

INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety — Hardware design requirements for computer-based systems, Rep. IEC 60987, IEC, Geneva (2007).

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Standard 7-4.3.2-2003, IEEE, New York (2003).

computer program. (See also software below.) A set of ordered instructions and data that specifies operations in a form suitable for execution by a digital computer. A combination of computer instructions and data definitions that enables computer hardware to perform computational or control functions.[4]

configuration management. The process of identifying and documenting the characteristics of a facility's structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation. 'Configuration' is used in the sense of the physical, functional and operational characteristics of the structures, systems and components and parts of a facility.

correctness. The degree to which a design output is free from faults in its specification, design and implementation. There is a considerable overlap between correctness properties and other characteristics such as accuracy and completeness.[5]

defence in depth. A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

dependability. A general term describing the overall trustworthiness of a system, that is the extent to which reliance can justifiably be placed on this system. Reliability, availability and safety are attributes of dependability.

design. The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems. Used as a noun, with the definition above. Also often used as an adjective, applied to specific categories of conditions or events to mean 'included in the design basis', as, for example, in design basis accident, design basis external events and design basis earthquake.

design basis accident. Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

diversity. The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure. Examples of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity), different sizes of equipment, different manufacturers, and types of equipment that use different physical methods (which provide physical diversity).

electromagnetic compatibility. The ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment.[6]

---

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety — Software Aspects for Computer Based Systems Performing Category A Functions, Rep. IEC 60880, IEC, Geneva (2006).

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Glossary of Software Engineering Terminology, IEEE Standard 610.12, IEEE, New York (2002).

[5] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electropedia: The World's Online Electrotechnical Vocabulary, IEV Ref. 161-01-07 (1990), http://www.electropedia.org.

embedded software. (See also firmware below.) Software (stored in read-only memory) that is built into a computer dedicated to a predefined task. Normally, embedded software cannot be modified by the computer that contains it, nor will power failure erase it; some computers may contain embedded software stored in electrically erasable programmable read-only memory, but changing this memory typically requires a special sequence of actions by maintenance personnel.[7]

equipment qualification. Generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements.

error. A human action or process that produces an unintended result.[8]

failure. The structure, system or component is considered to fail when it becomes incapable of functioning, whether or not this is needed at that time.

fault. A defect in a hardware, software or system component. Failures result when some condition (e.g. signal trajectory) triggers a fault.[9]

formal methods. Mathematically based methods for the specification, design and production of software. Also includes a logical inference system for formal proofs of correctness and a methodological framework for software development in a formally verifiable way.[10]

functional requirement. A requirement that specifies a function that a system or system component must be capable of performing. (Note: Software functional requirements are usually defined in the software requirements specification document, see IEEE 830-1993[11].)[12]

functionality. (As a software functional characteristic.) Those operations that must be carried out by the software. Functions generally transform input information into output information in order to affect the reactor operation. Inputs may be obtained from sensors, operators, other equipment or other software. Outputs may be directed to actuators, operators, other equipment or other software.[13]

hardware. Physical equipment used to process, store or transmit computer programs or data.[14]

interface. A shared boundary between two functional units, defined by functional characteristics, signal characteristics or other characteristics, as appropriate. (Note: The concept includes the specification of the connection of two devices with different functions.)[15]

---

[7] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Control Systems to Improve Nuclear Power Plant Reliability and Efficiency, TECDOC-952, IAEA, Vienna (1997).

[9] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Requirements for Coping with Common Cause Failure (CCF), Rep. IEC 62340, IEC, Geneva (2007).

[10] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

[11] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for Software Requirements Specifications, IEEE Standard 830-1993, IEEE, New York (1993).

[12] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

[13] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

[14] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Glossary of Software Engineering Terminology, IEEE Standard 610.12, IEEE, New York (2002).

[15] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electropedia: The World's Online Electrotechnical Vocabulary, IEV Ref. 351-42-25 (2013), http://www.electropedia.org.

logic. The generation of a required binary output signal from a number of binary input signals according to predetermined rules, or the equipment used for generating this signal.

microprocessor. (See 'computer' above.)

normal operation. Operation within specified operational limits and conditions.

operable. A system, subsystem, train, component or device is operable when it is capable of performing its specified safety function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication and other auxiliary equipment that are required for the system, subsystem, train, component or device to perform its specified safety function(s) are also capable of performing their related support function(s).[16]

physical separation. Separation by geometry (distance, orientation, etc.), by appropriate barriers or by a combination thereof.[17]

postulated initiating event. An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

programmable logic controller. A programmable logic controller is a digital device that is designed and used for automatic process control on the basis of a predefined, preprogrammed and preloaded control algorithm that functions on the basis of a very strictly defined sequential logic scheme.

protection system. A system that monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.

protective action. An intervention intended to avoid or reduce doses to members of the public in emergencies or situations of chronic exposure.

redundancy. Provision of alternative (identical or diverse) structures, systems and components, so that any one can perform the required function, regardless of the state of operation or failure of any other.

reliability. The ability of an item to perform a required function under given conditions for a given time interval. (It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval. Generally, reliability performance is quantified using appropriate measures. In some applications, these measures include an expression of reliability performance as a probability, which is also called reliability.)[18]

safety. The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards.

safety action. A single action taken by a safety actuation system. For example, insertion of a control rod, closing of containment valves or operation of the safety injection pumps.

---

[16] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

[17] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Electropedia: The World's Online Electrotechnical Vocabulary, IEV Ref. 395-07-125 (2014), http://www.electropedia.org.

[18] NTERNATIONAL ELECTROTECHNICAL COMMISSION, Electropedia: The World's Online Electrotechnical Vocabulary, IEV Ref. 192-01-24 (2015), http://www.electropedia.org.

safety actuation system. The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system.

safety function. A specific purpose that must be accomplished for safety.

safety group. The assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded.

safety related system. A system important to safety that is not part of a safety system. A safety related instrumentation and control system, for example, is an instrumentation and control system that is important to safety but it is not part of a safety system.

safety system. A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents. Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some plant operational states and non-safety functions in other operational states.

security. The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

self-test. A test, or series of tests, performed by a device upon itself. A self-test includes on-line continuous self-diagnostics, equipment initiated self-diagnostics and operator initiated self-diagnostics.[19]

severe accident. Accident conditions more severe than a design basis accident and involving significant core degradation.

software. Programs (i.e. sets of ordered instructions), data, rules and any associated documentation pertaining to the operation of a computer based instrumentation and control system.[20]

software life cycle. Necessary activities involved in the development and operation of software during a period of time that starts at a concept phase with the software requirements specification and finishes when the software is withdrawn from use.[21]

surveillance testing. Periodic testing to verify that structures, systems and components continue to function or are capable of performing their functions when called upon to do so.

traceability. The degree to which each element of one life cycle product can be traced forwards to one or more elements of a successor life cycle product, and can be traced backwards to one or more elements of a predecessor life cycle product.[22]

---

[19] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

[20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer Based Systems Performing Category A Functions, Rep. IEC 60880, IEC, Geneva (2006).

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer Based Systems Performing Category A Functions, Rep. IEC 60880, IEC, Geneva (2006).

[22] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Rep. NUREG-0800, NRC, Washington, DC (2014).

validation. The process of determining whether a product or service is adequate to perform its intended function satisfactorily.

verification. The process of ensuring that a phase in the system life cycle meets the requirements imposed on it by the previous phase.

ABBREVIATIONS

ANSI	American National Standards Institution
AOO	anticipated operational occurrence
ATWS	automatic trip without scram
CCF	common cause failure
CDA	critical digital asset
CFT	channel functional test
CIM	component interface module
CPLD	complex programmable logic device
DAS	diverse actuation system
DMZ	demilitarized zone
DPS	diverse protection system
DSD	diversity seeking decisions
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EPRI	Electric Power Research Institute
ESFAS	engineered safety features actuation system
ESPS	engineered safeguards protective system
FPGA	field programmable gate array
HDL	hardware description language
HPD	hardware description language programmable devices
HSI	human–system interface
I&C	instrumentation and control
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
ISA	International Society for Automation
ISM	industrial, scientific and medical
ISO	International Organization for Standardization
IV&V	independent verification and validation
KINS	Korea Institute of Nuclear Safety
MDEP	Multinational Design Evaluation Programme
MIMO	multiple input, multiple output
NPL	non-programmable logic
NRC	Nuclear Regulatory Commission
NuPAC	Nuclear Protection and Control
OLM	on-line monitoring
PIE	postulated initiating event
PPS	primary protection system
PRA	probabilistic risk assessment
PRPS	primary reactor protection system
R&D	research and development
RFI	radiofrequency interference
RM	requirements management
RPS	reactor protection system
SER	safety evaluation report
SSCs	structures, systems and components
SST	software statistical testing
SyRS	system requirements specification
V&V	verification and validation

CONTRIBUTORS TO DRAFTING AND REVIEW

Anikanov, S.	Westinghouse, United States of America
Eiler, J.	International Atomic Energy Agency
Friedl, M.	AREVA NP, Germany
Glöckler, O.	International Atomic Energy Agency
Hamar, K.	Hungarian Atomic Energy Authority, Hungary
Harju, H.	VTT Technical Research Centre of Finland, Finland
Johnson, G.	International Atomic Energy Agency
Kim, D.	Korea Institute of Nuclear Safety, Republic of Korea
Koskela, M.	Radiation and Nuclear Safety Authority (STUK), Finland
Lojk, R.	Canadian Nuclear Safety Commission, Canada
Oh, S.H.	Korea Institute of Nuclear Safety, Republic of Korea
Quinn, E.	Technology Resources, United States of America
Rounding, A.	AMEC, United Kingdom
Scott, C.	Schneider Electric, United States of America
Sohn, S.	Korea Electric Power Corporation, Republic of Korea
Takala, H.	Radiation and Nuclear Safety Authority (STUK), Finland
White, A.	Office for Nuclear Regulation, United Kingdom
Wood, R.	Oak Ridge National Laboratory, United States of America

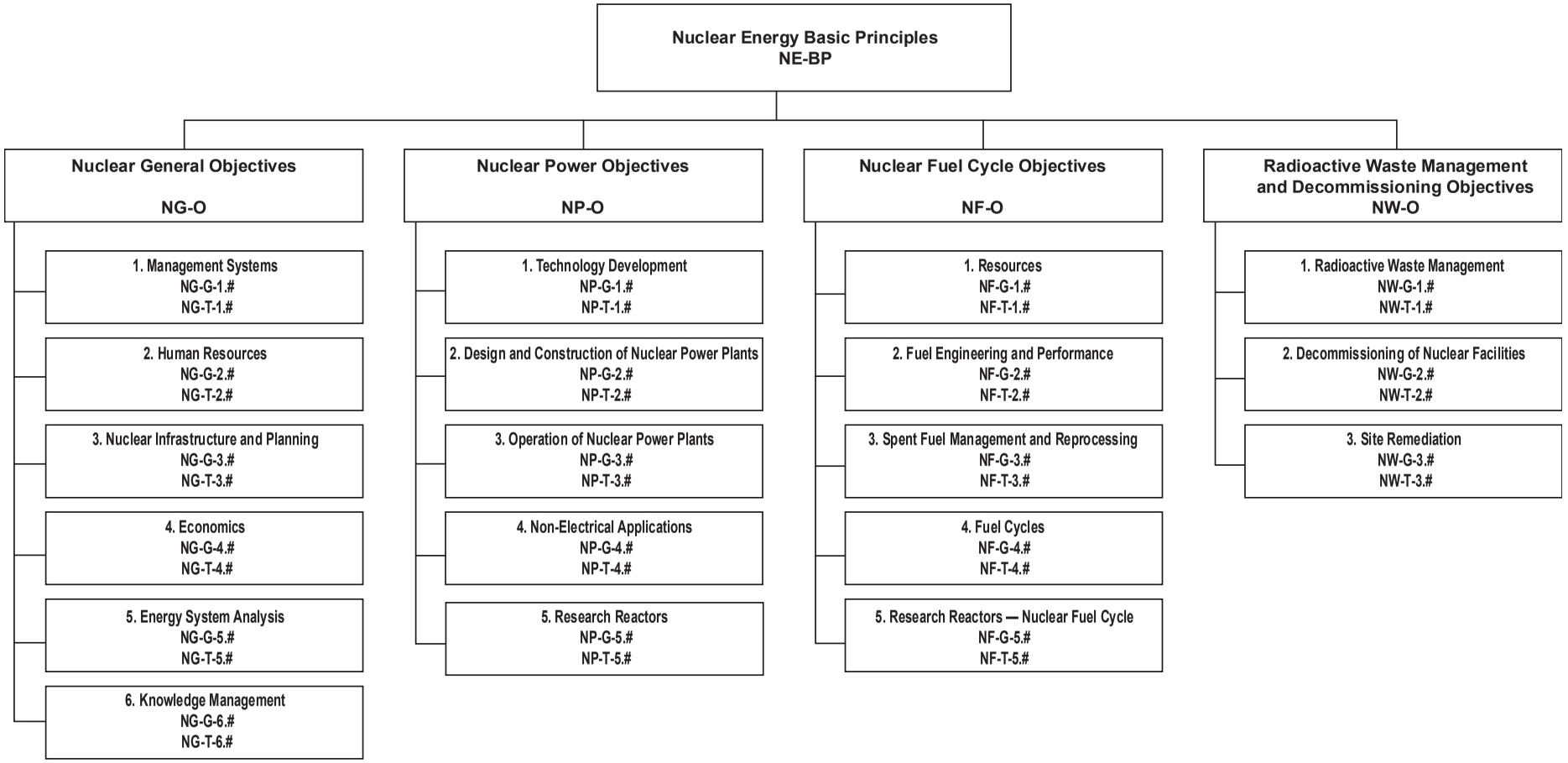
Consultants Meetings

Vienna, Austria: 3–6 November 2009, 17–20 May 2010, 11–14 March 2014

Technical Cooperation Workshop

Portoroz, Slovenia: 11–14 May 2010

Structure of the IAEA Nuclear Energy Series



Key

BP: Basic Principles
O: Objectives
G: Guides
T: Technical Reports
Nos 1-6: Topic designations
#: Guide or Report number (1, 2, 3, 4, etc.)

Examples

NG-G-3.1: Nuclear General (**NG**), Guide, Nuclear Infrastructure and Planning (topic **3**), **#1**
NP-T-5.4: Nuclear Power (**NP**), Report (**T**), Research Reactors (topic **5**), **#4**
NF-T-3.6: Nuclear Fuel (**NF**), Report (**T**), Spent Fuel Management and Reprocessing (topic **3**), **#6**
NW-G-1.1: Radioactive Waste Management and Decommissioning (**NW**), Guide, Radioactive Waste (topic **1**), **#1**

IAEA
International Atomic Energy Agency

No. 24

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.
Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

BELGIUM

Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA

Renouf Publishing Co. Ltd.
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC

Suweco CZ, s.r.o.
SESTUPNÁ 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FRANCE

Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 43 43 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: s.dehaan@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY

Librotrade Ltd., Book Import

Pesti ut 237. 1173 Budapest, HUNGARY
Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN

Maruzen Co., Ltd.

1-9-18 Kaigan, Minato-ku, Tokyo 105-0022, JAPAN
Telephone: +81 3 6367 6047 • Fax: +81 3 6367 6160
Email: journal@maruzen.co.jp • Web site: http://maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety

107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: http://www.secnrs.ru

UNITED KINGDOM

The Stationery Office Ltd. (TSO)

St. Crispins House, Duke Street, Norwich, NR3 1PD, UNITED KINGDOM
Telephone: +44 (0) 333 202 5070
Email: customer.services@tso.co.uk • Web site: http://www.tso.co.uk

UNITED STATES OF AMERICA

Bernan Associates

4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.

812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders for both priced and unpriced publications may be addressed directly to:

IAEA Publishing Section, Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

15-37681

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–102915–7
ISSN 1995–7807