IAEA Nuclear Energy Series

No. NP-T-2.11

Approaches for Overall Instrumentation and Control Architectures of 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.

APPROACHES FOR OVERALL INSTRUMENTATION AND CONTROL ARCHITECTURES OF 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
BARBADOS
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
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
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
SAINT VINCENT AND THE GRENADINES
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
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-2.11

APPROACHES FOR OVERALL INSTRUMENTATION AND CONTROL ARCHITECTURES OF NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2018

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/books

Printed by the IAEA in Austria
August 2018
STI/PUB/1821

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Approaches for overall instrumentation and control architectures of nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2018. | Series: IAEA nuclear energy series, ISSN 1995–7807 ; no. NP-T-2.11 | Includes bibliographical references.
Identifiers: IAEAL 18-01174 | ISBN 978–92–0–102718–4 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Instruments. | Nuclear reactors — Control. | Nuclear power plants — Safety measures. | Automatic control.
Classification: UDC 621.039.56 | STI/PUB/1821

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.

This publication concerns approaches for establishing the overall instrumentation and control (I&C) architecture of a nuclear power plant. The overall I&C architecture is defined herein as the organization of the complete set of I&C systems important to safety. Historically, the first generations of nuclear power plants relied largely on analogue I&C systems that were generally physically separate, hardwired collections of discrete components forming narrowly defined systems of independent functionality. Since the 1990s, digital technology has been increasingly employed through upgrades and new designs, leading to I&C architectures with more intercommunication and integration compared with these previously independent, isolated I&C systems. The movement to more comprehensive digital I&C architectures poses challenges such as preserving independence to support defence in depth, limiting the potential effects of postulated common cause failures, ensuring sufficient computer security and avoiding unnecessary complexity. Recognizing the relevance of these issues and the rapid development of technology, the IAEA's Technical Working Group on Nuclear Power Plant Instrumentation and Control recommended the drafting of this publication to elaborate I&C architectural approaches for its Member States.

This publication provides an overview of current knowledge, best practices and benefits and challenges related to the overall I&C architecture of nuclear power plants. Specifically, it describes the characteristics and content of general overall I&C architectures for nuclear power plants, presents general architectural principles, describes an architectural development process and discusses technical considerations for the design of an overall I&C architecture. The publication addresses issues concerning the organization of the complete set of I&C systems important to the safety of nuclear power plants; consequently, it does not focus on detailed technical information specific to individual I&C systems. The publication emphasizes safety aspects, but also includes consideration of plant availability, operability and security. This publication is intended to be used by Member States to support the design, development, implementation, operation and, as necessary, licensing of the subject systems.

The publication was produced by a committee of international experts and advisors from several IAEA Member States. The IAEA wishes to acknowledge the valuable assistance provided by the contributors and reviewers listed at the end of the publication, especially the contribution made by T. Nguyen (France) as the chair of the authoring group. The IAEA officer responsible for this publication was J. Eiler of the Division of Nuclear Power.

EDITORIAL NOTE

This publication has been edited by the editorial staff of the IAEA to the extent considered necessary for the reader's assistance. It 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.

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

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 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

The overall instrumentation and control (I&C) architecture of a nuclear power plant is the organization of the complete set of I&C systems important to safety. This organization includes, but is not limited to, systems identification, classification and segmentation, system and subsystem communication pathways, overall system and subsystem functions and signal handling. Therefore, this publication mainly concentrates on overall safety issues such as support of the 'defence in depth' concept and limitation of the potential effects of postulated common cause failures (CCF). It also addresses security issues, albeit in a more cursory manner, mainly by providing references to IAEA publications on security and by focusing on how such issues directly impact I&C architectural considerations and overall safety rather than on how an individual system would be designed or built.

Though individual system architectures are not, strictly speaking, parts of the overall I&C architecture, they are included in the scope of the publication when segmentation into subsystems places particular constraints on the inputs to the overall I&C architecture. The publication also recognizes the potential for adverse effects of I&C failures on plant availability and operability that may arise from increased architectural complexity; measures taken to ensure the essential features of the architecture (such as the independence of the levels of defence in depth) need to be considered as an integral aspect of the architecture as it is developed, with due consideration of their benefits and drawbacks.

Finally, the publication emphasizes the fact that the development of an overall I&C architecture could place demands on other aspects of plant design, such as plant nuclear design, mechanical or functional architectures, operators' roles and actions, electrical systems or cable routing. Experience suggests that two-way interaction between the design disciplines may help to optimize the I&C functionality and features that are required to be implemented so as to avoid unnecessary architectural and system complexity, which may in turn affect costs, operation and plant safety and availability.

This section provides background, describes objectives, defines scope and presents the publication's structure.

1.1. BACKGROUND

Units built before the 1990s relied on analogue I&C systems. These systems tended to be functionally independent arrangements with little communication between I&C subsystems and with human–system interfaces (HSIs) composed of dedicated hardwired displays. When these systems were designed, formal descriptions of defence in depth were not yet defined. Nevertheless, defence in depth concepts were incorporated into the analogue systems, but the approaches taken did not always match current guidance on the application of defence in depth.

Digital I&C systems important to safety were introduced gradually, either in the initial design or as upgrades. In many cases, the early digital I&C systems were obliged to conform to the conventional analogue architecture in terms of form, fit and function. Digital I&C systems for more recent evolutionary and advanced nuclear power plants have introduced architectural changes to allow greater connectivity and integration among previously separate and distinct systems. Nowadays, for a variety of reasons, digital I&C systems play an increasing role in nuclear power plants. All new designs depend in large part on digital systems and their software, and most I&C upgrades of existing units rely on programmable technologies.

The new systems have many advantages compared with older analogue based solutions, such as improved operational efficiency (e.g. due to the ability to operate closer to plant limits while maintaining adequate safety margins) and improved equipment monitoring and I&C self-monitoring. However, there has been an associated list of common challenges with digital I&C systems that the industry continues to debate and struggle with even today [1]. These include uncertainty and differences in developing and licensing digital I&C systems and equipment, and management of technical complexity arising from the enhanced functionality, highly integrated (and interdependent) architectures, widespread communications and flexible configurability that can be enabled by digital technology. Eventually, the benefits of expanded capabilities may be compromised by being too complex. Furthermore, as these digital systems are increasingly becoming more important to the safe operation of nuclear power plants, they are also correspondingly more vulnerable from a computer security standpoint owing to their interconnectivity.

The IAEA has issued Design of Instrumentation and Control Systems for Nuclear Power Plants (IAEA Safety Standards Series SSG–39, hereafter referred to as SSG-39) [2]. It provides guidance on the overall I&C architecture in support of the concept of defence in depth applied in the design of the plant systems and in establishing defence in depth for the I&C system itself as protection against CCF. This publication will complement SSG–39 [2] and will elaborate on some specific areas of design and implementation in a more detailed, practical manner.

1.2. OBJECTIVE

The goal of this publication is to assist Member States in understanding I&C architectural approaches and the benefits and challenges of the various methods for the design of nuclear power plant overall I&C architectures. It provides an overview of the current knowledge, up-to-date best practices, experiences, benefits and challenges related to the use of the subject approaches in the life cycle of I&C systems and the overall I&C architecture of nuclear power plants.

The publication is intended to be used by Member States to support the design, development, implementation, operation and, as necessary, licensing of the subject systems. 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 addresses issues concerning the organization of the complete set of I&C systems important to the safety of nuclear power plants. It does not generally address issues that are specific to individual I&C systems, many of which are covered by other IAEA Nuclear Energy Series publications. However, this publication does include some discussion of individual system design issues when they may have an impact on the overall I&C architecture. In covering the features of overall I&C architectures, the publication emphasizes safety aspects, but also includes consideration of plant availability, operability and security.

The information presented in this publication may be useful to support decisions in new plant designs and in modernization of existing operating nuclear power plants. This publication expands on the more general guidance found in IAEA safety guides, particularly in IAEA SSG–39 [2].

In presenting key considerations in the establishment of an overall I&C architecture for a nuclear power plant, this publication discusses an approach to developing an overall I&C architecture that involves a two-step process to facilitate agreement among stakeholders, regulatory approval and design optimization. As warranted, the publication provides guidance regarding the strengths and drawbacks of the different means of addressing key architectural issues.

Since the publication is intended to provide general information on architectural approaches rather than prescribe detailed solutions, it does not recommend specific approaches from standards bodies or particular stakeholders. Where appropriate, general examples are provided to illustrate concepts and references to relevant guidance documents are indicated to serve as resources for the target audience. However, it is recognized that there can be other variations in terms of the I&C designs, relative to the examples presented.

This publication is intended for all personnel involved in the design, development, manufacture, verification and validation, operation, maintenance and, as necessary, licensing of I&C systems at nuclear power plants. The following are foreseen as users of the new publication:

— Research and development organizations;
— Manufacturers and vendors;
— Technical support organizations;
— Regulatory bodies;
— Utilities and licensees.

1.4. STRUCTURE

This publication contains six main sections, including Section 1. Section 2 defines what an overall I&C architecture is, summarizes recommendations from relevant IAEA Safety Standards Series publications and describes the characteristics and content of general overall I&C architectures for nuclear power plants. Section 3 presents general architectural principles. Section 4 describes a structured process to develop an overall I&C architecture. Section 5 discusses technical considerations in the design of an overall I&C architecture. Section 6 summarizes the main technical observations made in this publication.

2. DESCRIPTION OF OVERALL I&C ARCHITECTURES

2.1. WHAT IS AN OVERALL I&C ARCHITECTURE?

The term ‘overall I&C architecture’ refers to the organizational structure of the I&C systems (components at the overall level) important to the safety of a nuclear power plant. It gives a high level view of the individual I&C systems and how they relate to one another. Often, non-classified I&C systems interconnected with I&C systems important to safety are also included in the overall I&C architecture. The overall I&C architecture also specifies the physical locations of the I&C systems (or of their constituent subsystems), and their dependencies on support systems such as power supplies and heating, ventilation and air-conditioning.

The primary functions assigned to I&C systems involve protection, control and monitoring. They are derived from the plant design basis and consideration of design extension conditions and sense basic physical parameters, monitor performance, integrate information and make automatic adjustments to plant operations as necessary. They also respond to failures and abnormal events, thus ensuring that goals of efficient power production and safety are met. Multiple I&C functions can be implemented within an individual I&C system. At the overall I&C architecture level, the purpose assigned to an I&C system may be quite broad, with further functional decomposition taking place as the detailed system and subsystem architectures are developed.

As mentioned in the introduction, the architecture of an individual system is not, strictly speaking, a part of the overall I&C architecture. However, it is taken into consideration when subsystem arrangements place particular constraints on the inputs to the overall I&C architecture design process, or when it is part of the diversity strategy to address digital CCF vulnerabilities [3].

Physically, an I&C system is composed of electrical, electronic and/or programmable electronic components, whose purpose is to perform defined I&C functions, as well as any service and surveillance functions that are necessary for the operation of the system itself. The elements within the boundary of an I&C system can include the processing and logic equipment, internal power supplies, sensors and other input devices, data highways and other communication paths and interfaces to actuators and other output devices. Many of these elements are dedicated to one system but some may be shared among several systems.

For new plant designs, development of the overall I&C architecture starts during the plant conceptual design. Certain architectural decisions need to be made early on, such as:

— The number of levels of defence in depth to be provided;
— The degree of independence required between levels;
— The manner in which non-classified systems will be separated from systems important to safety;
— The number of independent channels to be provided for safety systems;
— The degree of separation required between safety channels.

In this phase, I&C designers must make certain that plant designers allocate sufficient space for I&C cabinets, instrument racks, expected support equipment such as heating, ventilation and air-conditioning systems and instrument cable runs, and that the plant designers provide for sufficient separation between systems and subsystems expected to be independent of one another. Inadequate I&C involvement at this stage can result in problems for the future design.

From the conceptual design onwards, the overall I&C architecture will evolve from a continual discussion with other disciplines, e.g. plant layout, mechanical design, nuclear design, process design, human factors design, operations planning and computer security. As the plant design moves from general ideas to concrete designs, I&C engineers must continually evaluate the implications of other disciplines' decisions for the I&C design, work with these other groups to avoid unnecessary burdens being placed on the I&C design, and make the other disciplines aware of what is needed from them to support the ongoing development of the overall I&C architecture.

Often, the I&C architecture is not completely static. For example, additional subsystems (e.g. engineering workstations, tester units, or set point change or calibration devices) may be connected and subsequently disconnected at particular times (e.g. during outages) or for particular purposes (e.g. for periodic proof testing, equipment calibration or set point changes, or to modify functionality). Such aspects need to be considered with respect to the overall architecture as well as within individual systems to ensure that such facilities have adequate controls in place (such that systems can still perform their necessary safety functions when such subsystems are connected) and that they do not form a route by which multiple levels of defence in depth can be affected via the same or similar problems (e.g. miscalibration, electrical damage or security compromise).

Computer security needs to be kept in mind from the very start of developing an overall I&C architecture; this will help architects avoid architectural security flaws that can be very expensive to fix after the initial architecture is in place.

One of the challenges with respect to securing overall I&C architectures is to ensure that the implementation of any computer security measures does not impact other vital functional aspects of the I&C systems. For example, when using a traffic monitoring device to detect and signal abnormal communication patterns over a data communication path, it is important to make sure that no credible failure mode of the device can interfere with the data traffic.

2.2. GUIDANCE ON OVERALL I&C ARCHITECTURES PROVIDED IN IAEA SSG–39

SSG–39 [2] describes the overall I&C architecture as the organizational structure of the multiple plant I&C systems, each playing specific roles. The safety guide amplifies the description of the overall I&C architecture by indicating the items the architectural design establishes (Ref. [2], para. 4.1):

"— The I&C systems that comprise the overall architecture;
— The organization of these systems;
— The allocation of I&C functions to these systems;
— The interconnections across the I&C systems and the respective interactions allocated and prohibited;
— The design constraints (including prohibited interactions and behaviours) allocated to the overall architecture;
— The definition of the boundaries among the various I&C systems."

IAEA SSG–39 [2] also states in para. 4.4 that the "overall I&C architecture and the individual I&C system architectures should satisfy the plant requirements, including requirements for system interfaces and requirements for properties such as safety, security, verifiability, analysability and timing constraints."

Regarding the design of the overall I&C architecture, SSG-39 [2] states in para. 3.11 that the "design basis identifies functions, conditions and requirements for the overall I&C and each individual I&C system." This is one of the inputs that form the basis for the safety categorization of functions and their assignment to systems of the appropriate safety class. SSG-39 indicates that the overall I&C architecture design should result from the systematic allocation of required functionality and consideration of other requirements, such as those related to security zones, qualification, and reliability and availability goals.

An architectural feature given particular importance in SSG–39 [2] is defence in depth, and it stresses that the concept of defence in depth should be defined for the overall I&C architecture. Requirement 7 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1) [4] that levels of defence in depth be "**independent as far as is practicable**" is cited in SSG-39, para. 4.1, as an essential element of establishing defence in depth within the overall I&C architecture. Specifically, defence in depth is attributed to independent levels of defence such that one level of defence can compensate for the failure of another level.

Development of diversity strategies is also emphasized, diversity being one of the possible means to limit the potential of CCF among the levels of defence in depth within the overall I&C architecture. A hazard analysis is recommended to identify conditions that may compromise provisions for defence in depth or the diversity strategy adopted.

2.3. MAIN OVERALL I&C ARCHITECTURE PRINCIPLES

An overall I&C architecture is designed based on, and justified relative to, a number of key principles, as follows:

- Grouping of I&C systems into levels of defence in depth (see Section 2.5), so that if a failure occurs at one level, it is compensated for or corrected by other levels without causing harm.
- Categorization of function and system classification (see Section 3.3), according to their importance to safety.
- Placement of functions and systems in security zones (see Sections 2.6 and 3.4), according to their importance to security.
- Independence among levels of defence in depth and among safety classes (see Sections 3.2 and 5.2), so that:
  (a) An event that adversely affects one level, together with its consequences, does not reduce the effectiveness of the other levels in performing their functions important to safety;
  (b) An event that adversely affects an I&C system, together with its consequences, does not affect the effectiveness of systems that are more important to safety in performing their functions important to safety.
- Integration in, and consistency with, the plant architecture and concepts (see Section 3.5), in particular for safety (including defence in depth), security and operation, as the implementation of the principles may place specific constraints on the plant nuclear, mechanical and functional design.
- Elimination of unnecessary complexity and the location of necessary complexity where it can be best controlled (see Section 3.6).
- Appropriate location and protection of I&C equipment against hazardous environments (see Section 3.7).

These principles are presented in Sections 2.4–2.9 and then discussed in more detail in Section 5. Many also apply to the architectures of individual I&C systems and subsystems.

2.4. I&C SYSTEM LAYERS

The I&C system interfaces with plant operators and with the plant itself. This leads to the concept of I&C layers, which has been introduced by several publications (see Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12 [3]; the Electric Power Research Institute report on Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments [5]; and the American National Standards Institute and International Society Of Automation publication on Enterprise-control System Integration [6]). Note that computer security needs to be addressed in all layers and is a holistic aspect of the system rather than a specific processing layer.

Figure 1 shows the elementary layers of I&C, each of which has functional and communication capabilities.

- Layer 0 consists of sensors and actuators.
- Layer 1 comprises the devices that forward information from the sensors to the process control layer (signal conditioning) and/or that manage the actuators (priority management and actuator control).
- Layer 2 comprises the I&C systems required for the automation of the process and safety functions. In comparison with the other layers, a more rigorous justification of independence is expected between Layer 2 equipment and systems belonging to different levels of defence in depth. At the other layers, the needs for independence may be different (for example, although some conditioned sensor signals may be shared between more than one level of defence, the defence in depth in such cases may be provided by the use of

different and independent sensors that detect different plant conditions associated with individual abnormal plant events) but the defence in depth measures and independence will still need to be justified.

— Layer 3 (Supervisory control and information) comprises the I&C subsystems used for operating and controlling the nuclear power unit by staff in the control rooms.
— Layer 4 (Technical management) comprises the systems used for the technical management of the plant. Their functions are usually not important to safety, and therefore, provided that adequate independence measures are taken to ensure that they cannot adversely affect the equipment and systems in the other layers, they are outside the scope of the present publication.

Systems or devices in each layer may have dedicated HSIs. However, the main HSI for the supervision and control of the plant is in Layer 3. It generally includes workstations and control panels situated in the main control room and possibly in a supplementary control room.

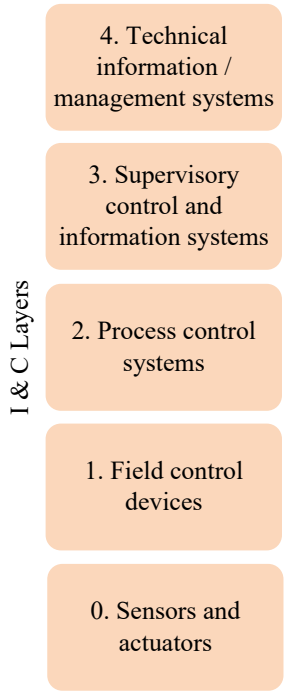


FIG. 1. Concept for instrumentation and control layers.

2.5. I&C LEVELS OF DEFENCE IN DEPTH

The requirement for defence in depth, as established in SSR-2/1 (Rev. 1) (Requirement 7 [4]), is discussed in greater detail in Section 3.1, but in its simplest architectural form, it can be conceived as different levels of systems as shown in Fig. 2.

Broadly, these levels prevent accident progression via a series of independent systems that perform different functions, such that failure at one level does not prevent the other levels from performing their functions. Typically, the functions performed at each level are as follows:

— Level 1: Plant control under normal conditions;
— Level 2: Monitoring for abnormal conditions and providing associated control functions;
— Level 3: Reactor trip and actuation of engineered safety features (e.g. to remove decay heat);
— Level 4: Monitoring and mitigation of severe accidents;
— Level 5: Monitoring of radioactive releases.

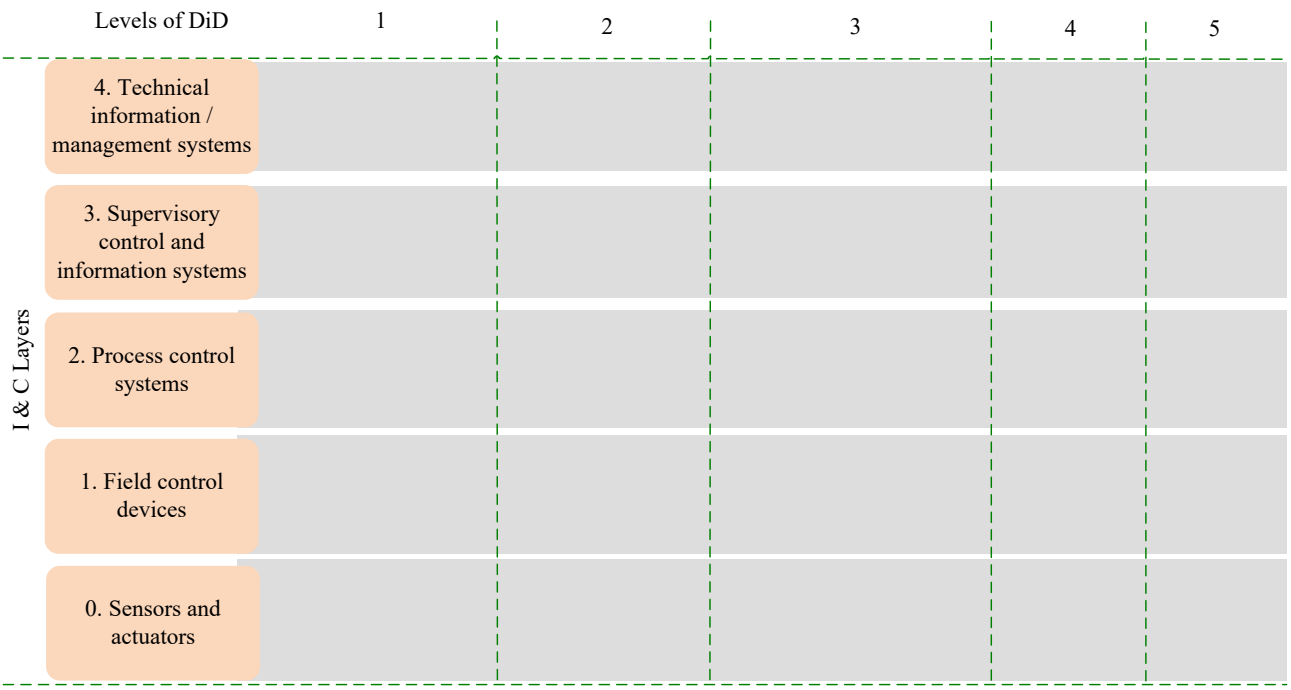


FIG. 2. Generic concept of levels of defence in depth. DiD — defence in depth.

Each of the systems in each level may have dedicated components associated with some or all of the I&C system layers, but it is possible that some levels may not include components at all layers (e.g. a very simple manual system might not include an automatic process control element, but might simply comprise controls and displays directly connected to field control devices). It is also possible that there is more than one I&C subsystem for some levels (e.g. it is not unusual to see a main protection system at Level 3 being backed up by an independent and diverse actuation system to further reduce risk in the potential event of protection system failure).

2.6. SECURITY CONCERNS AND ZONES

Computer security is generally concerned with five specific attributes: confidentiality, integrity, availability, non-repudiation, and authentication and authorization. Of these, the most important in I&C systems are integrity, availability, and authentication and authorization. Confidentiality, very important in traditional computing systems with a data management focus, is not as important for I&C, which simply does not handle data of lasting sensitivity when removed from an operational context. Likewise, though non-repudiation is important from an auditing perspective and to enable control system forensics, it is not as important as other attributes with immediate functional implications.

Availability concerns are usually addressed by defence in depth levels and approaches, whereas integrity concerns can be addressed by ensuring as far as is reasonably possible that information flows from security zones of higher integrity into security zones of lower integrity and not the other way around. Thus, I&C architects need to define security zones early in the architecture development process. These zones define partitions with differing information integrity needs, and are important to have in hand when architects begin to outline functions and data flows. This way, they can assign functional relationships such that integrity can be maintained by functions based on zone assignments.

However, it may not be possible in all cases to avoid information flow from security zones with lower security needs into security zones with more stringent requirements. When this is the case, the information in question needs to be pre-processed to ensure it can be trusted and it has not been corrupted. That said, these kinds of flows are best avoided whenever possible.

2.7. INPUTS TO OVERALL I&C ARCHITECTURE DESIGN

The design of an overall I&C architecture is based on a number of inputs provided by different engineering disciplines. It needs to be consistent with and justified with respect to inputs that generally include the following:

— The plant's overall design, and in particular the plant level concepts for operation, maintenance and testing, for safety, especially for defence in depth, for security, and more generally, for dependability;
— Human factor constraints for I&C and operator interfaces;
— Regulatory requirements to be satisfied;
— Computer security attributes such as data integrity, monitorability, etc.;
— Specification of the I&C functions to be implemented;
— Attributes of system quality, such as maintainability and upgradability.

Even though these are designated 'inputs to the overall I&C architecture design', in practice, it is highly preferable that I&C designers engage the other plant designers and planners to let them know the needs and constraints (be they regulatory, operational or technical) of I&C. In many cases, the most appropriate solutions do not lie in I&C or solely in I&C, but result from interdisciplinary approaches in which each discipline contributes where and when it is the most efficient, and when it is not too late or too costly. (See the discussion in Section 3.5.)

In general, full development of plant specific inputs takes time, and final, detailed inputs are available only late in the plant design process. It is highly preferable not to wait until then to initiate the I&C design process. In particular, the overall I&C architecture design could typically be initiated with partial and/or preliminary inputs that are gradually elaborated further and then completed.

Likewise, while the logical attributes of certain controls and subsystems can be initially analysed from a security perspective early in the architecture specification process, specific techniques and approaches to securing those controls will also likely shift during system implementation as well.

The functions identified as being required to respond to postulated initiating events (PIEs) are allocated to different systems in different levels of defence in depth as illustrated in Fig. 3. This process should not be understood to mean that there will be entirely separate systems for each level of defence in depth, or that a particular system is necessarily always used at the same level of defence. For example, it might be possible for an independent function to be implemented in the same technological system as the Level 1 normal process control system and to be used in support of accident mitigation at Level 4 or 5, or perhaps as a diverse backup to a Level 3 function. Indeed, at Level 4 there may be a limited number of designated I&C systems, but at this level, the general approach is to use anything that is working, potentially with additional flexible equipment.

This functional allocation to the levels of I&C defence in depth needs to be consistent with, and not challenge, the overall plant philosophy of defence in depth provided by the process systems. For example, functional diversity at the process level (i.e. at least two different ways of detecting an accident, and/or two or more different ways of responding to a potentially dangerous plant condition) offers the main defence against errors or misinterpretations of requirements or against unexpected conditions or unanticipated events. Equally, functions will be designated as either automatic or manual functions based on the best way to respond to the event (e.g. provision on an automatic function might impose unnecessary complexity) and on the time available for the response. This will also impact the I&C architecture design.

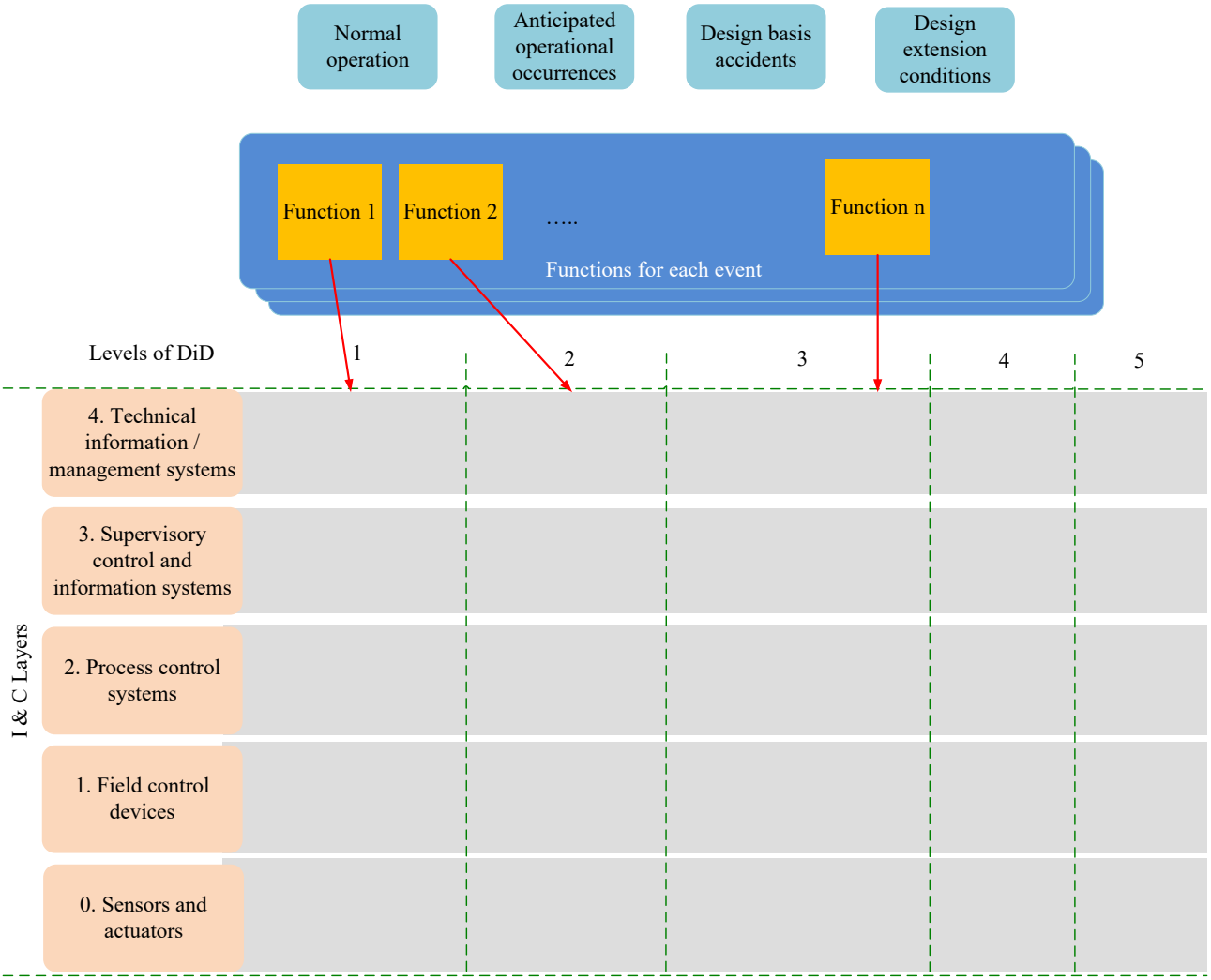


FIG. 3. Allocation of functions within an overall I&C architecture.

2.8. DIFFERENT CONTEXTS: NEW BUILDS AND MODERNIZATIONS

Modernization projects are part of the I&C life cycle. Hence, the life cycle of the I&C system can be divided into three major steps.

— The first I&C installation (new I&C project management in Fig. 4);
— I&C modernization and maintenance (I&C modernization management in Fig. 4);
— Decommissioning.

For new build projects, it may be appropriate to recognize these steps, given that long lives of 60 years or more are anticipated for new plants and it is likely, particularly for digital technologies, that I&C systems will suffer obsolescence issues. It is, however, unlikely that this will be an overall I&C architecture issue: it is more likely that obsolescence can be managed at the individual system level and by making provision to facilitate future modernizations (which may also require space within equipment rooms) and potentially also to support future plant decommissioning.

As compared with new build projects, the modernization of I&C in existing nuclear power plants generates some specific challenges. In a modernization project, only certain parts of the plant are directly concerned, and often the general concepts and design of the plant cannot be drastically changed. Furthermore, an overall I&C architecture already exists and often some elements of this architecture will not be changed. For example, it is quite common to make no or only limited changes to the Layer 0, and very often, new equipment and cables

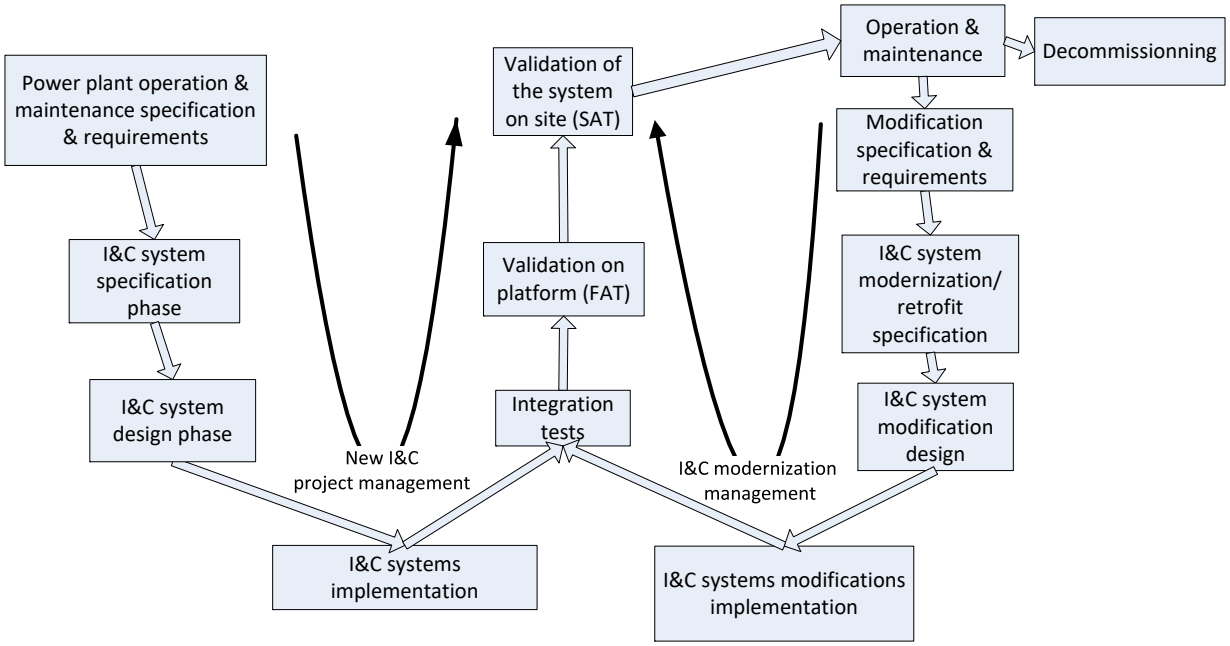


FIG. 4. I&C project management (reproduced from Ref. [3]). SAT — site acceptance testing; FAT — factory acceptance testing.

must fit into existing instrument rooms and cable runs. The issues created by such situations must be addressed (e.g. compatibility between new and existing equipment, issues caused by the installation of new systems such as different heating, ventilation and air-conditioning (HVAC) requirements for equipment loads, maintenance of allowed raceway fill and required separation between redundant systems and between voltage levels, justification for reusing equipment in a new context).

Furthermore, adding new digital components without appropriate system testing and profiling can and frequently does lead to new security vulnerability exposure. New equipment may introduce new features and services or may expose new functionality inadvertently. In either case, if a functionality is not needed (which is implied in the second case), it is to be deactivated if at all possible.

The I&C modernization could be realized through one or more of the following options:

(1) Spare part replacement;
(2) Form, fit and function module replacement;
(3) I&C rack replacement;
(4) I&C cabinet replacement;
(5) I&C systems modernization.

Option 1 requires no work on overall I&C architecture, as the existing function allocation and I&C design basis concept (including defence in depth) will remain valid.

The other options could require an update of the reliability, failure and hazard analyses of the overall I&C architecture, for example, when a digital component of a single design is applied in multiple I&C systems or multiple defensive layers to replace an analogue component.

For the last three I&C options above, it is necessary to distinguish between:

— One to one replacement of a single I&C system;
— Reassignment of several ‘process’ I&C systems to single I&C system(s).

The reassignment of several ‘process’ I&C systems to single I&C system(s) could introduce challenges to safety principles, such as defence in depth or diversity. However, even a one to one replacement could be a cause for concern. This is because, for instance, a diversity strategy (not considered in the original plant design) — internal or external to the system — might need to be considered.

For the last three I&C options above, the I&C design issues are different than for new builds. While the I&C design for a new build is either based on a well-documented generic design or developed on a blank canvas, all required information will be available for the I&C system realization. For I&C replacement projects, this kind of system specification is not always available. Extensive reengineering work needs to be performed in order to:

— Identify the required I&C functionality (platform independent);
— Assign the I&C functions to the related defence in depth level;
— Assign the I&C function to the appropriate security zone;
— Specify the needs for redundancy, segregation, separation, diversity, HSI, computer security, etc.;
— Identify existing system characteristics that may be important for the new design, but did not need to be defined for the original design (e.g. data refresh rate needs).

2.9. KEY ACTIVITIES

Besides the design activities that are directly related to the development of the overall I&C architecture, there are a number of key activities to consider:

— Vulnerability analysis and residual risk analysis;
— Justification of the designed overall I&C architecture;
— Continuing re-evaluation.

During the early stages of a plant design, a key input to establish the list of I&C functions important to safety is the plant level analysis of PIEs. This analysis defines the role that an I&C function may have to play either in leading to a particular event or in its progression. Depending on the frequency and the possible consequences of the initiating event and the role (preventive, mitigating, etc.) assigned to a particular function in response to that event, the function will be assigned to a particular defence in depth level and is given a certain safety category. It is important to note that the consideration of the beyond design basis events for digital CCF coincident with a PIE (either an anticipated transient or postulated accident) has a significant impact on overall I&C architectures.

Once the overall I&C architecture is established, it may be subjected to a deterministic safety analysis to verify and demonstrate that it is in compliance with a set of rules and acceptance criteria, and that multiple, independent layers of protection will have to fail before any harmful effects can be caused to the environment. It usually proceeds by postulating faults within the overall I&C architecture to identify points of vulnerabilities. These are areas where failures within the I&C systems, including software CCFs and single point vulnerabilities, could lead to undesirable plant consequences. To mitigate those, suitable design provisions may be added to the overall I&C architecture. Examples of such provisions could be added redundancy, diversity, separation by distance or barriers, safety measures within communication protocols, and so on.

Probabilistic safety assessment complements the deterministic analyses by determining the probability of failure for each of the systems that constitute the various barriers to the release of harmful effects. Its broader scope may help to resolve gaps that the deterministic analyses do not cover. The probabilistic safety assessment takes into consideration the frequency of initiating events (including spurious actuation caused by I&C system failures) and therefore provides security, risk and reliability insights that can support design decisions related to the overall I&C architecture. Thus, probabilistic safety assessment can identify the relevance of the main I&C systems in relation to other plant systems to ensure that the I&C architecture is not over or under-engineered relative to other parts of the plant.

Justification of the designed overall I&C architecture would address safety and/or security (for example, to support licensing, in particular regarding trade-offs), but also plant availability and efficiency (for example, to give adequate background information for future modernizations).

There must be continuing re-evaluation during plant development as details about plant and individual I&C systems become available, and during operation as significant events occur (e.g. failures in I&C or plant incidents or accident).

3. MAIN OVERALL I&C ARCHITECTURE PRINCIPLES

This section provides an overview of the principles that are pertinent to the realization of the overall I&C architecture to ensure that plant safety and performance objectives are met. These principles, first listed in Section 2.3, are discussed in greater depth accompanied by some specific examples in Sections 4 and 5.

3.1. DEFENCE IN DEPTH

The overall plant safety approach involves a defence in depth strategy such that multiple independent barriers fail before the public may be exposed to radiological consequences. SSR-2/1 (Rev. 1) [4], para. 2.12, states that:

> "this concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures."

The I&C systems, and in particular the overall I&C architecture, need to fit into this concept.

Different concepts and approaches for defence in depth have been published, based on lessons learned from experiences such as the accident at the Fukushima Daiichi nuclear power plant. Reference [5] provides an overview of the different concepts provided by the IAEA, the United States Nuclear Regulatory Commission and the Western European Nuclear Regulators Association (WENRA).

The IAEA defence in depth approach described in SSR-2/1 (Rev. 1) [4] identifies the five levels. From an I&C standpoint, they can be described as:

(1) The prevention of system failures and deviations from normal operations. This is a continuous and largely repetitive process. The algorithms used are very different from those of protection functions, and experience with the system functionality may be gained in every clock cycle. Also, the potential development of undetected failures can be lower.
(2) Control of deviations from normal operating states to prevent anticipated operational occurrences from escalating to accident conditions. This can be provided both by electronic means and by operator intervention, if there is enough time and information for such actions to be credited. The algorithms used are different from control.
(3) Protection (i.e. reactor trip and actuation of engineered safety features) to control and/or limit the consequences of accident conditions. This is based on demand and works very differently from control: real demands occur rarely, so there is little opportunity to detect hidden failures or to experience conditions that were insufficiently considered in the design. Therefore, the provision of a diverse means of protection is an important feature at this level.
(4) Severe accident management (i.e. monitoring and mitigation) to confine radioactive material. For this, a small set of highly robust instrument channels are needed. Additionally, the I&C system design needs to facilitate the operator's ability to use any relevant I&C functions available. Alternative means of actuating systems — needed to inject coolant, depressurize the reactor and maintain containment integrity — must also be considered. The possible need to support mobile means might also be considered.
(5) Emergency management (e.g. monitoring of radioactive releases) to mitigate the consequences of radioactive release. For this, the main functions are to understand what radiological materials are being released and in which direction. Many of these functions may be, and perhaps need to be, entirely separate from the overall I&C architecture.

In all cases, the defence in depth strategy involves a hierarchical deployment of different levels of protection to prevent the escalation of plant conditions as a result of anticipated operational occurrences or accidents. The strategy also has computer security implications.

3.2. INDEPENDENCE

SSR-2/1 (Rev. 1) (Requirement 7) [4] requires that the levels of defence in depth be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. It is generally possible to design and manufacture I&C systems that are highly independent from one another and to control the potential for CCFs. However, the practical limits to independence are often reached at the plant level, for example considering:

— The number of independent mechanical and electrical systems;
— The practical arrangements made for separating and isolating cable runs, sensors, actuators and equipment rooms;
— The organization of the support systems necessary to the proper operation of the I&C systems.

For example, an issue can arise where I&C signals from diverse systems come together when individual mechanical devices (e.g. components of the residual heat removal system) service multiple levels of defence in depth. Similar issues can arise where sensors need to be shared between levels of defence. There is no clear consensus on the best approach in these areas and such issues are currently being addressed on an ad hoc basis.

SSR-2/1 (Rev. 1) [4] emphasizes the need for independence between the features provided for design extension conditions, e.g. features at Level 4 for mitigating the consequences of accidents involving fuel melt, and those implementing protection functions at Level 3. The Fukushima Daiichi accident showed the importance of robust accident monitoring instrumentation at defence in depth Level 4 and the advantages of having simple means for ensuring core cooling and protection of containment that are independent of the plant itself.

Measures that can be applied to achieve independence include the following:

— Physical separation by distance, structural barriers or a combination of both.
— Electrical isolation by suitable application of design measures to ensure that an electrical fault in one system does not degrade a connected system, or by the use of redundant elements within a system.
— Functional independence where the successful completion of a system's required functions is not dependent upon any behaviour including failures and normal operation of another system, or upon any information derived from the other system.
— Independence from errors in data communication through the implementation of proper data communication network topologies (including absence of data communication between particular systems), technical means such as guaranteed one-way communication or deterministic data communication protocols and redundancy.
— Defence against CCF to reduce vulnerabilities in I&C systems at different levels of defence in depth to an acceptable level. Generally, it is accepted that the likelihood of CCFs resulting from design errors of hardware systems, e.g. pumps, motors, valves, equipment actuators and sensors, can be adequately controlled by effective design process rigour, quality assurance, surveillance and maintenance procedures.
— Independence of support systems.

Computer security also relies on separation to provide mitigation of the consequences of cyberattacks by means of physical and electrical isolation, as well as function and data processing isolation. The I&C design engineers need to ensure that the integrity of a system in a higher computer security zone is not jeopardized by dependencies on systems in lower computer security zones. Computer security zones are usually coincident with defence in depth layers, but they may not always be, and a single insecure data connection, incorrectly located, could undermine an entire zone.

3.3. CATEGORIZATION OF I&C FUNCTIONS AND CLASSIFICATION OF I&C SYSTEMS

The objective of categorization and classification is to facilitate a graded approach for the technical and quality assurance requirements of I&C systems important to safety. Also, a graded safety function categorization scheme helps identify and, as necessary, draw attention to I&C systems that are less important to safety but can contribute to or affect the implementation of safety functions.

An I&C function is assigned a safety category according to its importance to safety. This importance is determined by the consequences of its failure when it is required. In some safety function categorization schemes (e.g. IEC 61226 [7]), the consequences in the event of a spurious actuation and the contribution of the function to the prevention and mitigation of PIEs are also considered.

An I&C system and/or equipment is assigned a safety class according to the highest of the safety categories of the I&C functions it is required to implement. This classification determines the design and quality requirements for the I&C system and/or equipment, which in turn determine the required level of engineering process rigour to provide sufficient assurance that the I&C system and/or equipment meets the reliability and quality criteria to perform its safety functions.

3.4. COMPUTER SECURITY ZONES

IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [8], contains an example of one possible security zone structure, though this particular example is focused more on technology architectures than logical architectures. The zones need to be defined by specific risk based attributes. For example, following this model, computer security Zone 1 (or Level 1 as defined in Ref. [8]) would contain only the most sensitive systems. Other systems can be assigned to lower security zones as appropriate, with the lowest security zone containing office workstations. Normally, I&C systems will be in the highest two or three security zones, with other systems in the remaining zones.

When defining functional architecture and data flows, computer security zones need to consider data flows from zones of higher security into zones of lower security, not data flows in the opposite direction. Thus, I&C design engineers need to develop a computer security zone model prior to functional definitions and dataflow definitions to support appropriate categorization and to avoid inappropriate communication and trust propagation through a system.

Functions will ideally be classified at the lowest security zone possible. Over-classification, i.e. assignment of a function to a higher security zone than needed, incurs extra costs and can impose additional difficulty and inconvenience on operational staff.

3.5. INTEGRATION IN AND CONSISTENCY WITH PLANT ARCHITECTURE AND CONCEPTS

Plant architecture and concepts can provide many inputs to the overall I&C architectural design and it is important that this is not seen as a one-way flow. For example:

— The independence of I&C systems at different levels of defence in depth is not just a matter of overall I&C architectural design: operator actions and plant design features may also be an effective means of responding to CCF within the I&C.
— The overall I&C architecture needs to achieve functional independence among levels of defence in depth and computer security zones and this principle also applies to the specification of the I&C functions. For example, if a function allocated to one level of defence in depth needs an input from another function allocated to another level, then this defines a functional dependency between the levels of defence in depth. Similarly, if a function of a given safety category or computer security zone needs an input from another function of a lesser safety category or computer security zone, then this defines a degree of functional dependency that could be questionable. Therefore, it is preferable to avoid any such inherent functional dependencies when identifying and specifying the I&C functions. Where such a dependency is considered to be necessary, then it needs to be justified and documented in terms of why the dependency is necessary, how the receiving I&C function can be protected against failures of the sending I&C function, when the receiving I&C function would nonetheless be affected by a failure of the sending I&C function, what the worst case effects are and why these are acceptable (see Sections 4.4 and 5.2).
— Where I&C systems at different levels of defence in depth may control the same plant component, share the same sensor or be supported by the same support system (e.g. power, air, cooling, lubrication), failure of a

component, sensor or support system can often dominate the risk. Where a component is controlled by multiple I&C systems, there is a need to apply strong conflict resolution methods to offset any adverse effects.

3.6. ELIMINATION OF UNNECESSARY COMPLEXITY IN I&C

SSG–39, paras 6.1–6.291 [2], provides general recommendations for all I&C systems important to safety, suggesting in para. 6.1 that the "I&C systems should fully meet the requirements of their design basis" and, in para. 6.2, that "Unnecessary complexity should be avoided in the design of I&C safety systems." These two objectives can be difficult to reconcile while ensuring the right balance of measures for independence, diversity, operability and maintainability. It is good practice to identify and assess the benefits, drawbacks, challenges, consequences and constraints of a solution.

Generally, simplicity is desirable as it promotes understanding and verification, and reduces the potential for unexpected events or challenges. This is particularly the case for systems important to safety. Complexity can arise from functional requirements applied in I&C system designs and their architecture. For example, designers could, where practicable, avoid automating functions just because they can be automated when a manual control approach using less complex I&C technology offers a simpler and more flexible approach. Complexity can also arise from I&C architectural design decisions such as the use of diversity strategies to address digital CCF vulnerabilities, which can have a large impact on the I&C system architecture thereby creating complexity (e.g. more interfaces), unreliability (e.g. potential for spurious actuations) and human performance issues (e.g. the operator's perception about the status of the plant when two diverse systems are acting differently). The design of the overall I&C architecture needs to achieve an appropriate balance between the above factors by considering the approaches that can be adopted in relation to postulated I&C system design faults or challenges.

3.7. PROTECTION AGAINST HAZARDOUS ENVIRONMENTS

The I&C systems need to be designed to withstand the adverse effects from potential hazards that might occur in their operating environment. Such hazards might arise from external factors (e.g. tsunami, aeroplane crash, flooding or excessive ambient temperatures) or from internal events (e.g. fires, dropped loads or steam leaks).

Protection against both these sets of hazards is primarily achieved by installation in separate locations and physical protection within building structures of redundant I&C subsystems. The I&C systems need to be qualified (e.g. demonstrated by a combination of type testing and analysis) for the worst environmental conditions (e.g. temperature, humidity, seismic events, increased radiation) to which they may be exposed during operation while still being required to perform their safety functions. Finally, where I&C systems rely on essential support systems (e.g. power supplies, HVAC) to remain fully operable and within their specified environmental conditions, these must also cope with the anticipated external and internal hazards. These issues apply not just to automated elements of I&C systems, but to the entire I&C at all levels of defence in depth (i.e. including sensors, cabling and field devices) and the locations where personnel are required to interact with the I&C systems to perform safety functions (e.g. main control rooms and supplementary control facilities).

The I&C architecture design activity needs to be closely related to the overall plant design activity as the process systems must equally be protected against hazardous environments. The environmental protection philosophy will ensure that not only are all the components suitably qualified, but that redundant elements of I&C safety systems are adequately independent and physically separate. The same rigour may, however, not be needed to ensure independence between redundant elements of other levels of defence in depth (e.g. when a diverse backup system is used). The solutions adopted may not be the same at all levels of defence in depth for I&C systems architecture, but they need to be consistent with the overall plant philosophy and demonstrated to address the potential hazards that are anticipated.

4. DEVELOPMENT OF THE OVERALL I&C ARCHITECTURE

An overall I&C architecture can be subject to numerous constraints from multiple stakeholders, including designers, operators, platform vendors and regulatory requirements within Member States. These stakeholders can themselves be representative of many different disciplines, sometimes having differing viewpoints and conflicting requirements. The objective of this section is to describe the key elements of a multistep approach to developing an overall I&C architecture so that any conflicts and discrepancies can be identified before necessary design changes become too difficult or too costly to implement. Although not all regulatory bodies within Member States formally review preliminary or conceptual designs, a multistep approach can still be beneficial to designers.

— The design and development of complex systems is often split into defined steps such as preliminary design and detailed design: a well-organized process aligned to life cycle activities can assist in limiting the risk of design shortcomings and revealing any that may occur. It can also help in organizing the documentation and design justifications in a structured and more comprehensible way, which could assist in facilitating licensing applications.
— The end of each step is an opportunity to make sure that the different teams and disciplines can agree on a number of assumptions, decisions and features pertaining to the design and design basis of the overall I&C architecture. This is particularly important given that the overall I&C architectural design is an integral part of the overall plant design and that it may place constraints and requirements on other disciplines.

Sections 4.1–4.4 discuss the technical aspects of a notional two-step process. In practice, this does not need to be applied too prescriptively. Depending on circumstances, organizations may opt for a different balance between a two-step process or a process with more than two steps. Also, this publication does not address the period at the beginning of a project in which alternate design approaches are considered, often referred to as optioneering, and that leads to the firming up of conceptual I&C designs and architectures.

4.1. OVERVIEW

The design and development of an overall I&C architecture involves multiple engineering disciplines working together in a coordinated manner to implement processes and procedures set out in SSG–39 [2] (paras 2.1–2.167, The Management System for Instrumentation and Control Design). It involves safety, process and operations engineers defining key principles, high level requirements, main process features, safety and security concepts, as well as the general layout of an installation. The overall plant design is subsequently realized in practice by the multiple engineering disciplines and teams involved, including mechanical, electrical, civil and I&C engineering following a systematic approach and in conjunction with process systems, safety analysis and human factors teams (among others). Interaction between all engineering disciplines and teams is important throughout a development project to ensure consideration of all the requirements applicable to the overall I&C architecture.

In some circumstances, it can be possible to enable time and cost efficiencies in I&C design, in which some aspects of the work may be performed in parallel by the required stakeholders after decisions informing the overall I&C architecture have been made. In practice, the extent to which this may be possible is constrained by the I&C development life cycle which tends to limit parallel working to those design phases that provide functional assignments to individual systems within the overall I&C architecture. Exceptions can be planning activities to ensure that interactions with human factors and cybersecurity functions are taken into account during development of the overall I&C architecture.

According to SSG–39, para. 2.17 [2]:

“Three fundamental levels of life cycles are needed to describe the development of I&C systems:

(a) An overall I&C architecture life cycle;
(b) One or more individual I&C system life cycles;
(c) One or more individual component life cycles…”

SSG–39, para. 2.19 [2], provides an overview of a typical I&C life cycle, in which each phase or subphase may require input either from I&C life cycles (overall I&C architecture life cycle and/or individual I&C system life cycle), or from the life cycle of another discipline (e.g. process engineering and/or operational development). The verification of the outputs from each phase of the life cycle(s) as part of a quality plan is essential, as designs based on ambiguous conceptual descriptions might enable rapid progress at the beginning of a project, but can result in a need for modifications at a later stage. Also, SSG–39, para. 2.88 [2], states that I&C documentation should provide "… a means of communicating information between the various phases of and the various parties involved in the design process".

This quality plan is considered necessary to identify and verify the information and/or data required to execute the life cycle phase related activity (or activities) and to harmonize both the content of information and the time at which it may be shared between stakeholders.

Member States may have regulatory requirements for safety and security whose intent can potentially be interpreted differently, which can impact the design of the overall I&C architecture. Therefore, it is important that before determining a detailed architecture, a clear understanding of the regulatory requirements is in place. This can reduce the need for late architectural changes that often result in the addition of systems and equipment, which can cause the overall I&C architecture to be more complex than strictly necessary.

4.2. STEP 1: PRELIMINARY DESIGN OF THE OVERALL I&C ARCHITECTURE

In accordance with the guidance given in SSG–39 [2] (see paras 3.1–3.16, on the Design Basis for Instrumentation and Control Systems), the design of the overall I&C architecture needs to be aligned with the plant safety design basis documentation, taking into account fundamental information, which initially may be limited to the:

- Operating philosophy of the plant;
- Defence in depth concepts of the plant, including I&C and other relevant engineering disciplines;
- Safety functions to be provided by the overall I&C architecture;
- Safety categorization and the functional and performance requirements of the plant functions important to safety;
- Safety classification of structures, systems and components, including I&C systems within the overall I&C architecture;
- Non-functional requirements for properties such as safety, security and timing constraints;
- Security zone definitions, relationships and permitted interzone communication paths (these need to be outlined in a conceptual security model that provides and explains the rationale behind this information).

It is recognized that the detailed approach taken to function categorization, safety classification and interpretation of defence in depth levels may vary between Member States.

4.2.1. Objectives of Step 1

Step 1 results in the specification of the main features (see Section 4.2.3) of a preliminary overall I&C architecture. Carrying this out at an early stage in a project facilitates agreement between stakeholders. Also, where it may be necessary to make significant changes (e.g. to introduce additional safety functions), it is possible to limit the extent of reconsideration of design decisions. At this step, defined functions need to be assigned to defence in depth levels, safety category and security zones. The deliverables from this step include a collection of functions that describe the specific, high level missions of the system and how they are related. These functions are also initially assigned into security zones based on a conceptual security model provided as input to this phase.

The preliminary overall I&C architecture provides the design basis in terms of claims that are made on safety functions so that it can be used as, for example, a conceptual model, to facilitate the development of a final architecture. This needs to be kept as simple as possible to avoid introducing complexity into the design of the overall I&C architecture at an early stage in its development. In practice, there may be a need for flexibility in the architectural design at this step so that the detailed assignment of functions to I&C systems and subsystems at the

subsequent step does not require modification of the overall concept, given that some changes in the scope of the individual I&C systems may occur.

The documentation of this type of model needs to include the information necessary to identify the potential hazards that might result from the overall I&C architecture, along with the means to address them.

4.2.2. Inputs at Step 1

The information required at this first step relates to the identification of the requirements to be satisfied, such as those where the practices of specific Member States differ (see SSG–39, annex III [2]) or relating to specific I&C technology selection, and any constraints on the design. These design constraints can arise from the intended plant configuration and are, generally, predefined as part of the plant design and safety analysis.

The design constraints arising from the analysis need to include the identification and characterization of PIEs, including the:

— Identification of combinations of PIEs to be addressed;
— Defence in depth levels that address the PIEs;
— Response to each PIE;
— Allocation of safety functions to automatic or manual actions;
— Assignment of functions to security zones;
— Initial definition of required response times, accuracies and functional reliability targets.

Additionally, information obtained at this step from the identification of requirements and constraints may include the following:

— Principles that differentiate between the prioritization of automatic and manually initiated actions, and between automatic actions where, depending on the likely provision of instrumentation (i.e. sensors and actuators), more than one system can actuate a device or function;
— Requirements with respect to operational practices that have been assumed where the designer is not the nuclear power plant operator, including plant states, operational modes and shutdown conditions;
— Analysis of issues associated with I&C system technology selection in terms of safety and security functions at the plant;
— Operator information and control requirements and their allocation within defence in depth levels, including concepts for operation, maintenance and testing;
— Human reliability analysis;
— Discussions on the technical competence and training needs applicable to operators and maintainers of I&C systems within the overall I&C architecture;
— Design basis and design extension conditions;
— Proposed configuration of the process system under control and monitoring, such as configurations to ensure redundancy;
— Support systems, such as power supplies, instrument air and HVAC systems;
— Limitations imposed by the proposed plant layout for equipment installation and cable routing;
— Reliability targets for safety assumed in plant models, determined from the application of deterministic criteria and/or probabilistic safety assessment, and availability limits;
— Outlines of physical plant security requirements, systems and processes;
— Definitions of security zones and allowed security zone communication paths, including information on how to protect non-compliant controls or communications to support cases where interzone communication violates preferred pathways and communication rules;
— Environmental constraints determined by analysis of plant external and internal hazards;
— Operational experience regarding overall I&C architecture(s) from previous projects.

The approach applied to the conduct of plant operations in different plant situations (normal conditions (including shutdown), incident conditions without trip, incident conditions with reactor trip, accident conditions, severe accident and beyond design basis conditions) can lead to the identification of control rooms and control

room systems/workstations in each room. This can also influence the location of human–machine interfaces which can be present at one (i.e. Layer 3, supervisory control and information systems) or more (e.g. local to platform or equipment) I&C layers in a plant's defence in depth concept.

4.2.3. Outputs from Step 1

The design output from this first step will ensure that the concept for the overall I&C architecture is defined in terms of the functional characterization of defence in depth levels, security zones, (see Sections 2.6, 3.4 and 5.5) and layers (see Section 2.4), such that understanding and agreement on its validity can be achieved and a high level design safety justification can be made. This needs to include identification of the I&C systems and, where appropriate, devices allocated to a defence in depth level and their safety classification against reliability targets and deterministic criteria.

Note that sharing of devices between defence in depth levels needs to be justified to ensure that this is acceptable for safety (see Section 4.4). In particular, the justification could concern:

— Data or signal communication and device sharing between different defence in depth levels, as described in Section 4.4;
— Data or signal communication from a lower safety class to a higher one;
— Data or signal communication from a lower computer security zone to a higher one;
— Data or signal communication and device sharing that violate accepted communication paths as defined in the conceptual security model.

Support systems need to be considered (e.g. power supplies and/or HVAC for the I&C systems and equipment) as described in Section 5.2.2.5.

The architectural design rules need to be documented and typically will take the following into account:

— Functional safety categorization and systems safety classification (see Sections 3.3 and 5.4). It may also be necessary to consider seismic classification, depending on the proposed location for I&C systems within the plant.
— Separation in the sense of physical separation (see Section 5.2.2.1), electrical isolation (see Section 5.2.2.2), functional independence (see Section 5.2.2.3) and its application to I&C systems within either the overall architecture (see Section 5.2.2.4 for data communication) or support systems (see Section 5.2.2.5).
— Alignment of the overall I&C architecture with security requirements and potential impacts on plant availability, physical and computer security, and zones with defence in depth levels (see Section 5.5 for computer security).
— Risk assessments and impact analyses for computer security.
— Postulated I&C faults and failures (see Section 5.6).
— Requirements to support operations (e.g. testing, periodic testing, monitoring and maintenance as outlined in Section 5.9) and arrangements for reducing the potential for malicious actions (including spurious actuation) that can result in a hazardous plant condition.
— Arrangements that may need to be provided to facilitate future plant and I&C upgrades (see Section 5.10).
— Targets for software failure and CCF, where information regarding computer based platforms is available.
— Design requirements for severe accident I&C (see Section 5.1.1.2).
— Specification of any additional constraints on inputs to Step 2.
— Principles supporting the justification of any authorized exceptions (see Section 4.4.2).

Note that this last item comprises a rationale for any exception(s) to the architectural design rules to provide justification that an acceptable level of safety can be maintained.

4.3. STEP 2: DESIGN DEVELOPMENT OF THE OVERALL I&C ARCHITECTURE

4.3.1. Objectives of Step 2

The second step is the design development of the overall I&C architecture, which is expected to take place without significant changes or redesign following the understanding achieved on completion of the first step. This ensures that the preliminary overall I&C architecture determined by Step 1 is complied with during the development of the I&C systems or, alternatively, is updated as necessary. This phase also specifies the additional details that are necessary for the implementation of the individual I&C systems. The primary output from this step is a more granular functional breakdown of the original, more abstract functions. These new functions describe how activities introduced in the original high level functions are accomplished.

4.3.2. Inputs to Step 2

Similar to Step 1, inputs in terms of I&C system functional, security, and performance requirements and any constraints will be established with other engineering disciplines to ensure that their design basis is satisfied. This will normally include the following:

— The I&C functional specification (see Section 5.4). Details for each I&C function may be provided with the high level functions defined as an input to Step 1 and the detailed specification of the functions being further refined during this step to establish, for example:
  - Functional description (i.e. purpose);
  - Defence in depth level;
  - Safety category and system classification;
  - Inputs (including their sources) and outputs;
  - Separation/grouping with other particular I&C functions in the same defence in depth level and safety category;
  - Functional diversity for each PIE;
  - Prioritization criteria;
  - Operating modes, including any manual intervention and monitoring requirements in different plant conditions;
  - Logical operations and/or voting criteria, response time, accuracy, failure modes and effects analysis, behaviour of I&C system in response to faults.
— Justification of exceptions to design rules and constraints determined during Step 1 and a rationale as to why the exception is necessary.
— The conceptual security model used in Step 1.
— Justification that failure or compromise of one or more I&C functions does not prevent (e.g. through functional diversity or other design controls) a safe state being achieved or maintained at the plant. This needs to be justified in terms of any specific measures that are to be implemented to achieve this outcome.

4.3.3. Outputs from Step 2

The outputs from Step 2 will complete the definition and safety justification of the overall I&C architecture, and will normally include such outputs as:

— The selection and justification of I&C platforms and associated subsystems, system development methodologies and tools. A justification that these aspects of I&C system design and selection comply with the corresponding requirements established during Step 1 needs to be provided.
— The overall architecture of I&C systems, including the identification of subsystems and human–system interactions and associated features to be provided in one or more control rooms, measures ensuring

independence, separation or segregation[1] in terms of both safety and plant availability, and safety classification of subsystems in accordance with the approach established during Step 1.
— The design of data or signal communication between levels of defence in depth and/or independent or separated subsystems, taking into account requirements to avoid, as far as is practicable, communication from lower to higher safety classified systems.
— An overall defence in depth and diversity analysis.
— The allocation of I&C subfunctions (after decomposition) to systems and subsystems, taking into consideration any constraints that are applicable to separation or grouping and platform capabilities. The allocation needs to be justified in terms of compliance with design rules and applicable specifications for response times and fault tolerance. Subfunctions, after this step, will also be assigned to specific security zones.

Any exceptions to design rules applied during development of the overall I&C architecture need to be justified in accordance with the advice provided within Step 1.

4.3.4. Phases within Step 2

The phases in Step 2 will be similar to those in Step 1, with collection of the inputs from other engineering disciplines, the development of a complete definition of the overall I&C architecture, and its safety justification, and, as necessary depending on the Member State, submission for regulatory acceptance. It is possible that the collection of inputs, together with the specification of requirements on individual I&C systems deriving from the overall architecture, will also proceed in a phased way with identification of I&C functions followed by their gradual refinement.

4.4. OVERALL I&C ARCHITECTURE DESIGN OPTIMIZATION AND JUSTIFICATION

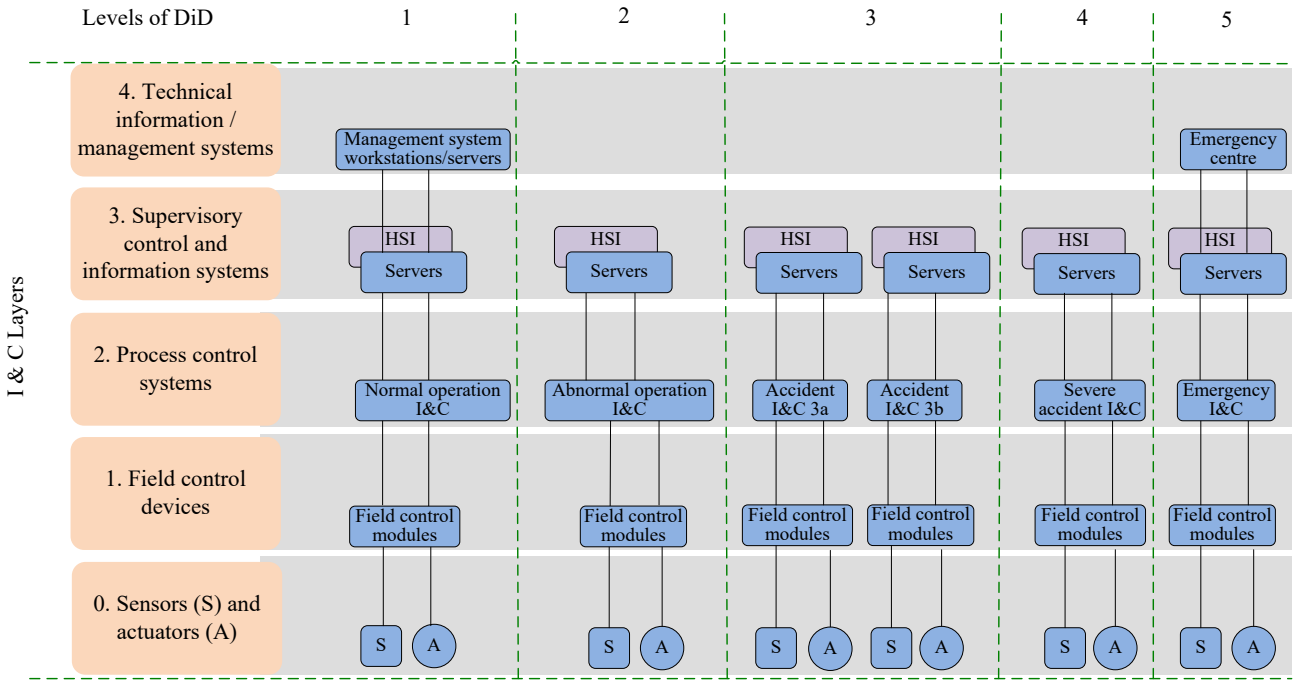
4.4.1. General

Figure 5 is a purely theoretical view of an overall I&C architecture aiming to achieve independence between layers of defence in depth, where each level of defence has its own instrumentation (sensors, actuators, field, etc.), its own I&C systems and its own HSI, and no data communication with the other levels. In addition, each level incorporates sufficient redundancy and/or diversity to reduce identified CCF vulnerabilities to an acceptable level.

This theoretical approach to overall I&C architecture design is often impractical or insufficient to reduce the likelihood of CCF between I&C systems in the various layers of defence in depth to an acceptable level, while also meeting the desired characteristics that support plant safety objectives, such as reduced complexity and improved operability and maintainability.

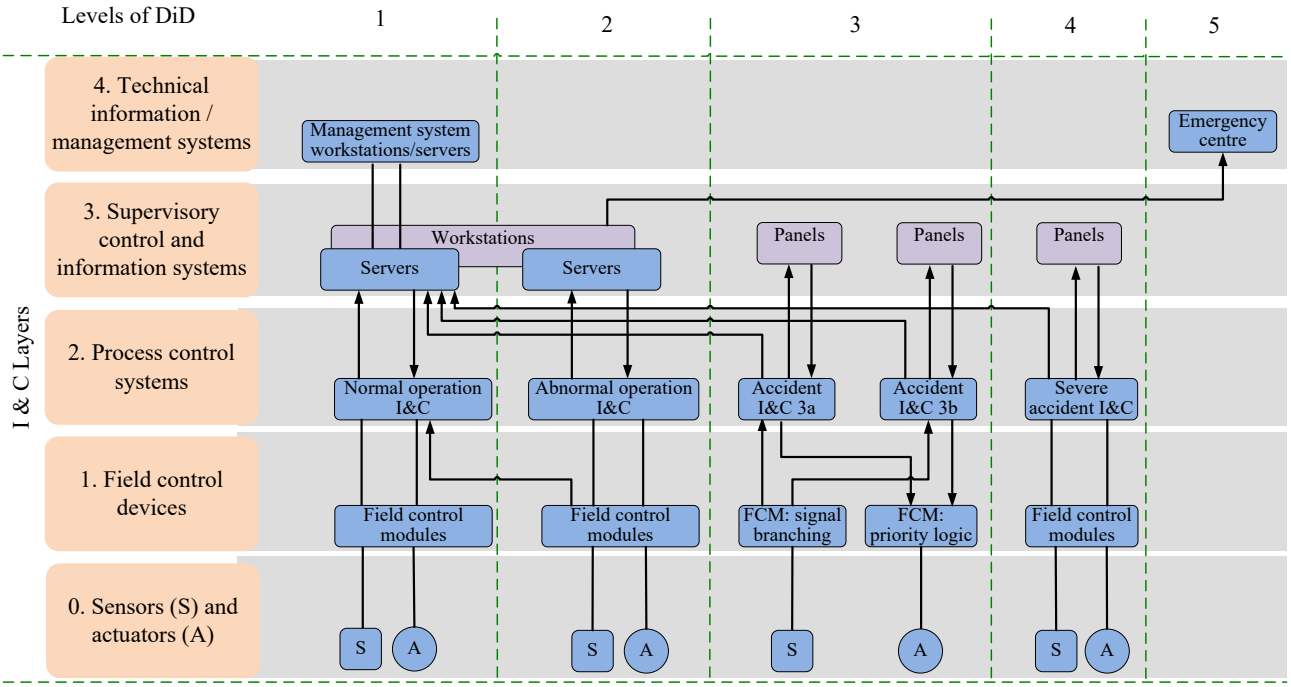
Figure 6 shows a hypothetical overall I&C architecture design that has been subject to optimization.When the optimization of an overall I&C architecture design is carried out, it is important to ensure that the fundamental requirements for the safety of a nuclear power plant are achieved and can be adequately justified. This justification needs to take account of and document any additional equipment and devices (e.g. signal conditioning devices allowing the sharing of a sensor signal among multiple systems, or priority actuation logic allowing the sharing of an actuator among multiple actuation sources).

[1] In accordance with the guidance provided in SSG–39 [2], defence in depth within the overall I&C architecture should be implemented by means of independent lines of defence, so that the failure of one line of defence is compensated for by the following one. For a safety system or systems within the overall I&C architecture, this should be achieved by using design principles of physical separation, independence, isolation from other systems, including safety related systems, and sharing no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other equipment at the nuclear power plant, which, in the event of a fault, might jeopardize the safe working of the safety system(s) within the overall I&C architecture.



HSI: Human-system interface

FIG. 5. An overview of an I&C architecture that is idealized in terms of the independence of its defence in depth levels.



FCM: Field control module

FIG. 6. A more realistic illustration of an overall I&C architecture.

4.4.2. Overall I&C architecture design justification

During optimization of the overall I&C architecture design, the following questions are normally asked:

(a) Is optimization really needed, i.e. do the benefits outweigh the disadvantages?
(b) Have all functional interactions been considered and what are the worst case consequences that can result from these interactions?
(c) Are the design provisions adequate, i.e. can the design provisions be fully relied upon to eliminate any unacceptable consequences of these functional interactions?
(d) Does the optimized design adequately satisfy its assigned safety functional requirements?

A structured and systematic approach is used to justify the optimized overall I&C architecture design to provide a documented design basis for it. The objective is to provide a clear description of the overall I&C architecture design in relation to the proposed optimized implementation and the basis for any decisions made to provide assurance that it can satisfy relevant safety functional guidance such as that provided in SSG–39, paras 4.1–4.40 [2].

In practice, there has been a trend towards an explicit claim-based approach to safety assessment and assurance, and considerable work has been done on the structuring of safety arguments [9–12]. The key elements of a claim-based approach applicable to optimization, as shown in Fig. 7, are:

— A claim can be considered an assertion put forward for general acceptance in relation to the safety of either the overall I&C architecture or I&C system(s). Typically, these are statements about a property of the architecture or systems.
— An argument is used to link the claim and supporting evidence.

Evidence is used as the basis of the justification of the claim. Sources of evidence can include the design, the development process, prior field experience, reviews, testing or analyses of various forms (e.g. deterministic, probabilistic, qualification). Further information on claim-based approaches can be found in Refs [9–12].

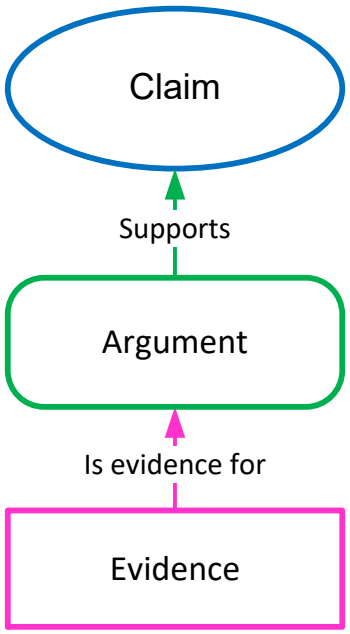


FIG. 7. Basic elements of a claim-based approach.

The following are examples of attributes of an overall I&C architecture design where optimization may need to be made and justified to ensure that safety functional requirements relevant to defence in depth layers are adequately satisfied.

4.4.2.1. The plant human–system interface design

The control and display connections within an HSI (in Layer 3) may require careful design to ensure the implementation of requirements for independence, separation and diversity while providing control room operators with a convenient and easy to understand user interface. The design of an HSI that deals with operator interface functions needs to recognize any limitations of plant operation due to control room staffing arrangements and requirements applicable to operator response in normal, abnormal and emergency situations. Also, in some cases, aggregation of information allows for a much better presentation of integrated alarm annunciation. The HSIs will be designed to also align with the security model. Usually, this involves allowing information display in multiple locations but command issuance only from specific systems. For example, information from a high security zone could be displayed anywhere, but commands sent to that same security zone generally come only from a system in the same (or higher) zone.

The use of multiple HSIs belonging to the different levels of the plant defence in depth model will need to be addressed as part of human factors assessments and part of the operational training requirements to ensure that there are no detrimental effects on safety in all plant conditions.

4.4.2.2. Sharing of instrumentation and actuators

It may be necessary to share instrumentation or actuators between multiple levels of defence in depth. In such cases, evidence that adequate redundancy and/or diversity has been applied and that there are design provisions in place to ensure that there can be no cross links that can defeat multiple levels at the same time is needed. These design measures provide the basis for the evidence that the cross links have been minimized. As an example, the electrical isolation of a shared signal may be used so that a failure of a non-safety system cannot be propagated to a safety system. This isolation device needs to be associated with the safety system and needs to be classified and qualified accordingly. It will normally be justified that the periodic testing of the safety system channels would not impact the reliability or effectiveness of, for example, the process control system. Similarly, it will be justified that a failure would not have an adverse impact on any aspect of the deterministic basis for safety, such as the single failure criterion (SFC), in the overall I&C architecture design. Similarly, it will not cause a significant increase in the frequency in demand (or spurious actuation) of the safety system.

4.4.2.3. Data communications

In cases where there is a need to have an integrated HSI, it may be necessary to have data communication across systems belonging to different levels of defence in depth, as well as systems belonging to different safety classes or security zones. In such cases, adequate, justified and accepted design rules will be used to ensure that such system configurations implement the fundamental requirements for independence and that these rules are rigorously followed and documented. Such rules may include the use of point to point communication, unidirectional communication from higher to lower security zones or higher to lower class I&C systems important to safety, separation of the safety logic execution process from the communication process, embedding safety properties into communication protocols to ensure coverage for all postulated communication faults, data validation at the receiving end, and non-interference arising from communication between I&C systems important to safety and non-classified I&C systems. Arguments to justify design optimization need to be complemented by an analysis of the consequences of postulated failures.

4.4.2.4. I&C platform diversity

In order to obtain adequate diversity among the different defence in depth levels and achieve a high level of protection against CCF, an overall I&C architecture design with different platforms in each level may be considered. However, in practice, such systematic diversity may be difficult to achieve and lower levels of diversity may be

adequate though, for example, diversity between the system(s) that may be postulated to fail owing to a CCF and the system or systems that are intended to provide a diverse backup might normally be provided. Arguments to support optimization decisions with respect to systematic diversity will be supported by hazard analysis of each postulated single event and combination of events as part of the overall I&C architecture design justification.

5. SPECIFIC TECHNICAL CONSIDERATIONS FOR THE DESIGN OF OVERALL I&C ARCHITECTURES

5.1. DEFENCE IN DEPTH

5.1.1. Levels of defence in depth

The IAEA Safety Glossary [13] defines defence in depth as:

"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*."

Defence in depth is implemented through design and operation to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the plant and events initiated outside the plant. The objectives are as follows:

— To compensate for potential human and component failures;
— To maintain the effectiveness of barriers by averting damage to the plant and to the barriers themselves;
— To protect the public and the environment from harm in the event that these barriers are not fully effective.

SSR-2/1 (Rev. 1) [4] identifies five levels of defence, which are summarized from an I&C standpoint in Section 3.1.

Different jurisdictions around the world may have somewhat varying interpretations of the levels of defence in depth defined by the IAEA. In this section, as an example, WENRA's interpretation proposed in their report on the Safety of New NPP Designs [14] will be discussed.

The interpretation from WENRA is summarized in Table 1. In particular, it proposes a refined structure of the levels of defence in depth that takes into account current international harmonization efforts, the trends regarding the specific issues raised by digital I&C systems and equipment, and the lessons learned from past accidents. This reference to the WENRA report [14] does not imply that its interpretation is the only possible one. Nevertheless, in subsequent discussions, the WENRA defence in depth concept is used as a frame of reference. It should be noted that Ref. [14] was published before SSR-2/1 (Rev.) [1] and that therefore all references in Table 1 are to the earlier, unrevised edition[2] of these requirements.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).

TABLE 1: LEVELS OF DEFENCE IN DEPTH ACCORDING TO THE WENRA REPORT ON THE SAFETY OF NEW NUCLEAR POWER PLANT DESIGNS *(adapted from Ref. [14])*

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3a[a]	Control of accident to limit radiological releases and prevent escalation to core melt conditions[b]	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact[c]	Postulated single initiating events
Level 3b		Additional safety features[d], accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features to mitigate core melt, management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response intervention levels	Off-site radiological impact necessitating protective measures[e]	

[a] Even though no new safety level of defence is suggested, a clear distinction between means and conditions for Sublevels 3a and 3b is outlined. The postulated multiple failure events were considered a part of the design extension conditions in the now superseded IAEA SSR-2/1.

[b] Associated plant conditions now being considered at defence in depth level 3 are broader than those for existing reactors as they now include some of the accidents that were previously considered 'beyond design' (level 3b). For level 3b, analysis methods and boundary conditions, design and safety assessment rules may be developed according to a graded approach, also based on probabilistic insights. Best estimate methodology and less stringent rules than for level 3a may be applied if appropriately justified.

[c] It should be noted that the tolerated consequences of Level 3b differ from the requirements concerning design extension conditions established in the now superseded IAEA SSR-2/1 that give a common requirement for design extension conditions: for design extension conditions that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary.

[d] The task and scope of the additional safety features of Level 3b are to control postulated CCF events as outlined in section 3.3 of Ref. [14] on Multiple Failure Events. An example for an additional safety feature is the additional emergency AC power supply equipment needed for the postulated CCF of the primary (non-diverse) emergency AC power sources. The task and scope of the complementary safety features of level 4 are outlined in section 3.4 of Ref. [14] on Provisions to Mitigate Core Melt and Radiological Consequences. An example for a complementary safety feature is the equipment needed to prevent the damage of the containment due to combustion of hydrogen released during the core melt accident.

[e] Level 5 of defence in depth is used for emergency preparedness planning purposes.

WENRA emphasizes independence between different levels of defence in depth, and identifies critical instances where it may be strictly enforced to the extent practicable, as follows:

— Particular importance is given to the independence of Level 3 from Levels 1 and 2.
— Sublevels 3a and 3b also need to be independent from one another.
— Level 4 needs to be independent from all the other levels to the extent reasonably practicable.

The benefits of defence in depth are clear: multiple independent barriers must fail before the public is exposed to a potential hazard. WENRA recognizes that enhanced defence in depth is a major evolution in: (i) the range of situations considered in the initial design to prevent accidents, to control them and to mitigate their consequences; and (ii) in the corresponding design features of the plant. Possible disadvantages of increasing the number of levels of defence in depth might be that:

— The large number of levels requiring independence from one another can increase complexity in the overall plant design, in some cases rendering certain aspects of the designs impractical. Therefore, overall I&C architectures will, in general, need to be optimized in some respects such as shared instrumentation, data communications and shared HSIs among defence in depth levels (see Section 4.4).
— More complex overall I&C architectures and systems may be more difficult to design, verify, operate, inspect, test and maintain. Also, more numerous defence in depth levels might lead to higher risks of spurious actuation. This could have an adverse effect on safety and plant availability.

5.1.1.1. Design basis conditions and design extension conditions (Levels 3 and 4)

It can be noted that the WENRA approach splits defence in depth Level 3 into two sublevels:

— Defence in depth Level 3a provides control of single PIEs.
— Defence in depth Level 3b provides control of multiple PIEs or failure events.

Thus, defence in depth Level 3b addresses the following:

— The combination of a single initiating event with the failure of defence in depth Level 3a. To address this type of situation, a backup system may be used that is diverse and independent from the main safety system in defence in depth Level 3a. This is often known as a diverse actuation system. A separate IAEA publication addresses the specific issues associated with diverse actuation systems [15]. The scope of such a system may be more limited than the scope of the main safety system when a consequence analysis (using best estimate techniques) shows acceptable results with no actuation.
— The combination of multiple initiating events, but with correct operation of defence in depth Level 3a.
— Events resulting from internal or external hazards beyond those already addressed by defence in depth Level 3a.

Even though the WENRA approach is provided only as an example, it is nonetheless representative of the general trend towards more inclusive protection: events or combinations of events that used to be considered ‘beyond design’ are now covered by design extension conditions. These are postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process with best estimate approaches.

Depending on the required scope of the defence in depth Level 3b systems and possibilities for design change, different solutions may be chosen, as illustrated in the following two cases.

(a) *Case 1: Existing plant*

The WENRA report is intended for new plant designs and is not necessarily applicable to existing plants. However, an upgrade project may decide to follow its recommendations to the extent practical. For example, it may not be possible to add independent sensors (e.g. detectors) and actuators for a backup to the main safety system of defence in depth Level 3a, but the I&C of defence in depth Level 3b could still provide a diverse actuation system (with appropriate field equipment for the sharing of sensor signals and priority

logic for actuator controls). This limited solution is still useful, as it provides defence against a postulated CCF of the redundant channels of the main safety system.

However, even though the objective of the new defence in depth Level 3b is to enhance safety, several issues need to be considered, such as:

— The increased risk of spurious actuation, which may have adverse effects on plant lifetime and safety.
— The possible need for more complex priority logic and for signal pre-processing due to the sharing of sensors and actuators: the effects of failure of such field devices may need to be taken into consideration as they might affect both defence in depth Levels 3a and 3b. The use of dual controls also results in the need to consider separate operating bypass and reset controls. These features also add complexity to the failure modes and effects analysis, since each system has to be considered working separately and then working simultaneously with the postulated single failures.

(b) *Case 2: New build in late design stage*

At that stage, it might be possible to extend the solution of Case 1 and, for example, provide independent sensors and diverse functionality for the backup I&C system allocated for defence in depth Level 3b. As with Case 1, one needs to consider the increased risk of spurious actuation and the possible need for more complex priority logic.

(c) *Case 3: New builds in early design stage*

In this case, designers may have more freedom in finding solutions avoiding or reducing the issues raised in Cases 1 and 2, for example, by a suitable allocation of diverse safety functions to the systems in defence in depth Levels 3a and 3b.

5.1.1.2. Robustness of severe accident I&C (defence in depth Level 4)

Several publications on post-accident monitoring have been issued by the IAEA, the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronics Engineers (IEEE). One of the latest and the most comprehensive of these is IAEA Nuclear Energy Series No. NP–T–3.16 [16]. It covers all the main relevant aspects such as selection of the parameter to be monitored and post-accident monitoring design and implementation. In particular, post-accident monitoring needs to be designed for operation in the conditions that can cause, or are created by, the severe accident, and which are likely to be more severe than those required of the other systems. The overall I&C architecture also needs to consider that:

— The I&C systems in defence in depth Levels 1–3 have failed to prevent the accident.
— They may have been damaged by the cause of the accident or by the accident itself.
— The support systems may also have been damaged.

5.1.2. Control rooms and workstations, displays and procedures

The plant operating staff are provided with display, alarm annunciation and supervisory control interfaces that enable them to monitor and control plant operations in different plant modes and take actions to ensure plant safety as necessary. These displays and controls comprise Layer 3 (supervisory and control information) as indicated in Section 2.4.

From an overall I&C architecture point of view, there are a number of issues that need to be addressed, such as:

— The allocation of functions to automatic I&C systems and to human operators: This task is typically performed by I&C and human factors engineering specialists, consistent with high level operational concepts and by addressing the functions defined by process and safety engineers. It is an input provided to the I&C specialists. It relates to questions around the reliance that the design places on humans to ensure safety, and also to the time available for humans to respond to faults and accident sequences. For example, some Member

States apply a 30 minute rule during which a manual action to ensure plant safety is not envisaged. However, while operators may not be the preferred first response to faults, staff can offer very flexible solutions to unexpected events and can make use of the full range of available monitoring and actuation facilities, which are not necessarily limited only to control rooms, but may also take place locally in I&C equipment rooms or at plant control devices (e.g. valves). Anticipated operator actions required to maintain safety in the event of faults need to be controlled via defined procedures that are formally linked to and justified in the plant safety analysis.

— Adequate defence in depth in the HSI: This is an overall I&C architecture question and relates to trade-offs between the conflicting objectives of end-to-end independence among each level of the I&C defence in depth architecture (e.g. independent HSI for each level), the benefits of simplicity, and the desire for operators to have all the available information in one place and in a common form. A typical trade-off might be to provide access to all information via the normal displays, which in turn requires design features to ensure that independence between levels of defence is maintained and that faults or malicious attacks cannot propagate between them (this is discussed in Section 5.2.2.4 on communications and Section 5.5 on computer security), but to provide the key parameters and controls that ensure plant safety via an independent HSI, and also to provide independent facilities for monitoring (and controlling where appropriate) severe accidents (e.g. as illustrated in Figs 5 and 6).
— Adequate defence in depth with respect to hazards: This task again involves inputs from process and safety engineers and relates to the need to provide different locations from which the plant can be monitored and controlled. For example, an internal hazard, such as a large scale fire, may be postulated such that it may be necessary to evacuate the main control room. In this situation, operators must be provided with sufficient facilities, preferably in a single location and protected from the hazard (e.g. in a different fire zone), to safely shutdown the reactor and to maintain it in that state, potentially for a significant period of time (e.g. following an extensive fire). The alternate or backup control facilities can include capabilities to cope with any faults or events that might occur as a result of the hazard (e.g. control must be transferred to the alternative location and switched away from the main control room so that the effects of fire cannot cause spurious actuations), or during shutdown operations. There is also likely to be a significantly separated location (i.e. a different building or site) from which the response to severe accidents can be made that is not subject to those same events or conditions (e.g. severe flooding or high radioactivity) that may have contributed to the accident or may be a direct outcome of the accident.

Regardless of how plant HSIs are mapped to the defence in depth levels, the design needs to be well-informed with the application of human factors engineering principles. This includes establishing guidelines for attributes that take into consideration human cognitive abilities and limitations on human performance, such as operator loading and operator response times, as well as those that deal with ergonomics, such as conventions for colour codes, labels and symbols.

5.2. INDEPENDENCE AMONG LEVELS OF DEFENCE IN DEPTH

The purpose of independence is to help ensure that the functionality realized in I&C systems and electrical equipment is not compromised by the same or concurrent failures. IEC 61513 [17] characterizes independence as design provisions that "prevent adverse interaction between subsystems of the system or with other systems which might result from abnormal operation or from failure of any component in either subsystem or system, including from common-cause failure." Essentially, independence is intended to avoid physical and logical interactions that can permit the propagation of failure effects and to minimize vulnerabilities to CCF. It is especially important to establish independence among levels of defence because these levels are intended to provide successive, compensating barriers to provide defence against escalating consequences of plant events.

Independence (including defence against CCF) among levels of defence in depth can be realized by separation (physical, electrical, functional, support resources) and/or diversity.

Considerations to address the characteristics of digital technology in establishing independence are identified below.

— Functions implemented in software or in software designed logic can include latent faults that could lead to systematic failures and, when triggered concurrently, to CCF.
— Arguments based on independence by virtue of protection provided by an operating system (e.g. control of access privileges) may be difficult to defend as they depend upon the reliability of the operating system software that enforces the separation.
— Computer systems that are physically separate may still interfere with one another logically through data exchanged over network or communication links.
— Criteria for functional independence and independence from the effects of communications errors can include:
  • No direct interaction based on buffering through shared memories;
  • Communication with other systems being only unidirectional (including no handshaking);
  • Software continuing to work regardless of network faults and communication processing being separate from the processing of the logic;
  • Input data from other systems being validated before use.

Errors in the design requirements for plant systems, I&C systems and operator training have also contributed to accidents. In fact, they have been the most fundamental causes of previous severe accidents [18]. The traditional approach to these concerns is to provide conservative designs and to operate the plant in a conservative manner. Nevertheless, errors in design requirements and training have had a large role in the most serious reactor accidents. The use of diverse systems, signals and functions to respond to events provides a measure of protection against errors in the requirements or analysis of I&C systems.

5.2.1. Defence in depth levels and postulated initiating events

The independence of defence in depth levels could be analysed considering each level as a whole. However, a generally accepted practice is to analyse the independence of defence in depth levels considering each PIE in turn, together with their associated preventive and mitigation measures. The objective of the analysis is to ensure that adequate defence in depth is available for each PIE, possibly taking into consideration the frequency of the PIE. The systems involved against each PIE may not always be the same and may not necessarily always respond to different PIEs in the same order.

5.2.2. Defence against failure propagation

According to IAEA SSR-2/1 (Rev. 1), Requirement 21 [4], "**Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.**" These means can be extended by the independence of support systems.

Figure 8 illustrates different measures for separation. Different measures should be applied as appropriate for their architectural realization.

5.2.2.1. Physical separation

According to the IAEA Safety Glossary [13], physical separation is defined as "separation by geometry (distance, orientation, etc.), by appropriate *barriers*, or by a combination thereof." Furthermore, a barrier is defined as "A physical obstruction that prevents or inhibits the movement of people, radionuclides or some other phenomenon (e.g. fire), or provides shielding against *radiation*."

Physical separation is a means to cope with mechanical or environmental impacts. Physical separation could be achieved by separation by distance, structural separation or a combination of the two, and is a means to reduce the likelihood of dependent failures (i.e. CCFs) resulting from failures as consequences of PIEs (such as fire, missile, flooding or high energy pipe break).

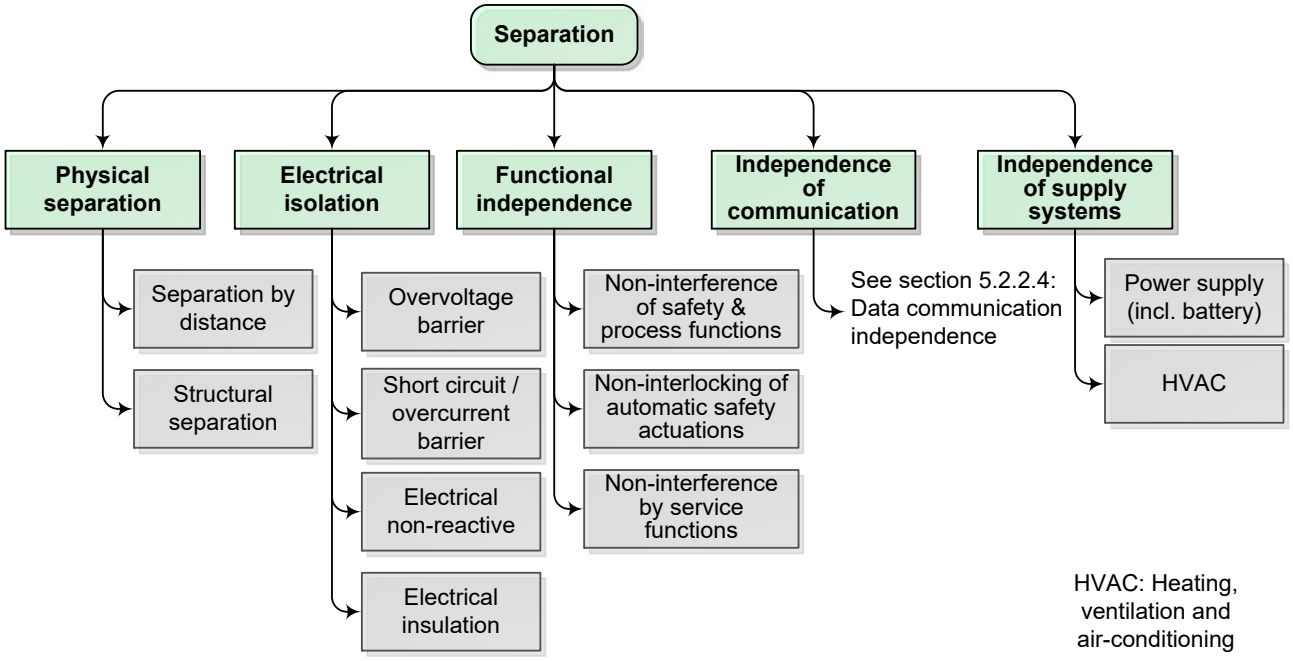


FIG. 8. Measures for separation.

The choice depends on the PIEs and may differ from location to location within the nuclear power plant. It will depend on the need to provide protection against all the PIEs considered in the design basis.

In some cases, full separation may not be practicable, and the layout design of some components may necessitate the installation of higher and lower classified circuits or different voltage levels (e.g. power supply and I&C check back signal) close together, such that the desired physical separation cannot be achieved. Dedicated measures are normally implemented in such cases to cope with postulated failures for the particular component.

5.2.2.2. Electrical isolation

SSG–39, para. 6.38 [2], states that "Electrical isolation is used to prevent electrical failures in one system from affecting connected systems or redundant elements within a system."

Furthermore, SSG–39, para. 6.41 [2], states that "Devices providing electrical isolation should prevent maximum credible voltage or current transients, grounds, open circuits and short circuits applied to one side of the device from unacceptably degrading the operation of the connected safety circuits."

These definitions could be summarized as: electrical isolation is used to prevent failure spreading via electrical interfaces.

An I&C or electrical system needs to be protected from or be tolerant to a faulty insertion of the system's own as well as foreign voltage or current (overvoltage barrier, short circuit or overcurrent) and ensure the integrity (electrically non-reactive, electrical insulation) of signal multiplication and transmission. Electrical isolation measures (decoupling concept) are identified in Fig. 8.

The identified isolation measures address different electrical effects, so selection among them for implementation involves consideration of the hazard(s) of concern. Based on the required use cases, a combination of measures can be specified in the design. Depending on the range of effects that could be present, omitting specific measures could compromise the effectiveness of the complete electrical isolation.

5.2.2.3. Functional independence

Functional independence between systems is defined by IAEA SSG–39, para. 6.44 [2], as "... a condition that exists when successful completion of a system's required functions is not dependent upon any behaviour, including failures or normal operation, of another system, or upon any signals, data, or information derived from the other

system.” However, assessment according to this definition can be performed only when enough information on the systems concerned is available.

Lack of functional independence could be intrinsic to the functions’ definition, when one or more of the required functions of the first system are by their own definition inherently dependent on the correct performance of one or more functions of the second system. Functional dependence could be introduced by data communication, which could be direct or indirect (via other functions or via shared resources).

When identifying and specifying the I&C functions needed by the plant, it is generally preferable to avoid intrinsic dependence between functions belonging to different levels of defence in depth. In the same spirit, it is generally preferable that functions important to safety or security are not intrinsically dependent on functions of lesser importance. When such situations cannot be avoided, it is good practice to provide a justification of why this is necessary or beneficial, and also a justification that this will not lead to unacceptable consequences in the plant (e.g. provision of adequate preventive or mitigation measures).

5.2.2.4. Data communication independence

Electrical isolation is only one of the aspects that needs to be addressed when using data communication links (whether point to point or multiplexed) across boundaries of defence in depth levels, or between I&C systems of different safety classes. One also needs to take into account more functional failure propagation modes such as transmission of incorrect values, absence of transmission, transmission overload or delays. These may be triggered by the data sender (e.g. by sending an incorrect value), by the receiver (e.g. by failing to send an acknowledgement if the communication protocol requires it), by another station connected to the communication link or by the communication link itself. The number and variety of these modes tend to increase with the complexity of the communication protocol.

For defence in depth, data communication independence is the ability of any defence in depth level to perform its functions important to safety or to reach a safe state regardless of the behaviour (correct or incorrect) of the other defence in depth levels with which it is connected, via one or more data communication links. For I&C systems design, data communication independence is the ability of any system to perform its functions important to safety or to reach a safe state regardless of the behaviour (correct or incorrect) of the other systems of lesser importance to safety or security with which it is connected, via one or more data communication links.

When the required functions of a system are all intrinsically independent from all the functions of another system, it is preferable to avoid altogether introducing data communication from the second system to the first, particularly when the two systems belong to different levels of defence in depth, or when the first system is of a higher importance to safety or security than the second. If data communication is justified, then it is preferable that it is limited to the minimum that is strictly necessary, and that adequate measures are taken on both sides of the communication.

Measures to prevent propagation of error or adverse effect may be determined on the basis of an analysis of how the communication could go wrong. This will depend on the design of the communication link(s). For example, with message based communication, there could be avalanches (too many messages that could overwhelm the receiver), spurious messages (messages received when none were warranted), silence (too few messages received), incorrect data, etc. Incorrect data could be non-plausible (i.e. detectable by the receiver by means of data validation) or worse, incorrect but plausible (hence not detectable by means of data validation).

Various measures may be taken to ensure data communication independence, which include:

— One-way data communication links, guaranteeing that senders cannot be affected by receivers or the data communication links. This could be obtained through the configuration of the data communication links, the data communication protocols, appropriate gateways, or hardware or physical means.
— Data communication protocols or data communication configurations guaranteeing a maximum (and acceptable) communication delay.
— Data communication protocols guaranteeing detection of communication errors (e.g. through the use of error detection and possibly correction codes) and message losses (e.g. by the sequential numbering of individual data communication messages).
— Fixed data communication network configurations, where the stations and the messages allowed in the network are specified during design.

— Redundant data communication links.
— Point to point data communication links: this could be used, for example, to minimize the extent of postulated failure propagation.
— Bandwidth bottlenecks (e.g. data communication filters, low bandwidth media) guaranteeing that no station connected to the link can generate unmanageable data communication storms.
— Data validation by the receiver, ensuring that non-plausible received values are discarded. In this case it should be noted that incorrect but plausible values may still be accepted by the receiver.
— Failure analysis, showing that failure propagation modes that cannot be completely prevented (e.g. reception of incorrect but plausible data, late data or absence of data) will not lead to inacceptable consequences.

The measures to ensure data communication independence also need to address computer security; see Section 5.5.

5.2.2.5. Support systems

Support systems provide the necessary conditions for the continued operability of I&C and electrical systems, including environmental control, power supply, instrument air and so on. Effective I&C system design will minimize the need for support systems and allow for the use of very simple support systems where needed. In general, the range of significance of support systems can be characterized as follows: (i) No support systems; (ii) support systems that are provided only to extend equipment lifetimes; (iii) support systems that are not necessary to support the performance of safety systems; and (iv) support systems that must be available to support the performance of safety functions.

In practice, it is difficult to eliminate the need for I&C systems to have an external electrical power source, but thoughtful design of the I&C system can eliminate the need for safety classified HVAC systems. Doing so may involve derating certain components, increasing the volume of equipment rooms or providing passive heat absorbing systems. Thus, cost trade-offs are involved, but these alternative approaches may, in the long run, be less expensive than the life cycle cost of active systems.

Instrument air systems commonly provide safety classified air receivers near instruments and valves needing air as an alternative to providing safety classified compressors and distribution systems.

IAEA SSR-2/1 (Rev. 1) [4], para. 5.43, requires that “it shall not be permissible for a failure of a support service system to be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions and compromising the capability of these systems to fulfil their safety functions.” This implies that where support systems are necessary, multiple system divisions with separation requirements similar to those applicable to the concerned I&C systems would need to be employed. Support system requirements are a result of I&C design, thus the type of support systems to be provided becomes a design constraint for the I&C system. Support systems would typically be controlled by dedicated hardwired or computer based controllers. These would be largely standalone with limited monitoring in the control room. The design would be such that the control of the support systems is not adversely impacted by the propagation of any external faults.

The design of a support system needs to ensure that its failures are not the dominant factor in the unavailability of a safety division. More generally, as support systems such as HVAC or power supply systems often support several I&C systems belonging to different levels of defence, the overall I&C architecture can incorporate provisions to ensure that they are not the dominant factor in the failure rates of I&C systems.

The pros and cons of separation measures for support systems need to be considered. In particular, strict separation could limit solutions to cope with postulated failures and come at the expense of availability. Decisions could be made based on probabilistic safety assessment insights.

As an example, dedicated and separated HVAC systems are installed for the different divisions, but in case of an HVAC failure in one division, ventilation flaps between divisions could be used to service the affected division. Even if the ventilation pipes lead to a certain level of dependency, this could improve availability, provided that appropriate defensive measures are taken, such as protecting against fire propagation.

To increase the availability of the power supply for I&C systems, a two-supply circuit could be considered in the basic design. Depending on the constraints for the architecture of the electrical power supply, the double feed-in could be realized by symmetrical or parallel power distribution (each division supplies itself, plus the additional supply) or by a duplex supply by its own division (buffered by battery or without battery) with the option to manually connect the power supply of two divisions.

The HVAC and power supply systems are usually essential to ensure safety during normal operation, and their failures can have a direct, adverse impact on safety functions. Thus, they usually need to be safety classified. However, as support systems affect the safe operation of I&C systems to different degrees and on different timescales, it is good practice for the safety classification to take into consideration the following factors:

— The time during which the I&C system is needed after a demand;
— The time during which alternative actions can be taken;
— The time needed to detect and remedy hidden failures.

5.2.3. Defence against common cause failure

5.2.3.1. Conservative design, construction, operations and maintenance

Conservative design, construction, maintenance and operation of I&C systems in accordance with quality management and proven engineering practices can achieve relatively high levels of quality for both hardware and software systems. The levels of reliability and safety of nuclear power plants can largely be attributed to these efforts.

Nevertheless, such approaches will never be perfect. Fundamental but subtle errors in system design requirements can be difficult to find during verification and validation. The United States Nuclear Regulatory Commission publications on Failures of General Electric Type HFA Relays in Use in Class 1E Safety Systems [19] and on Failure of Reactor Trip Breakers (Westinghouse DB–50) to Open on Automatic Trip Signal [20] provide well known examples, but a study of nineteen severe accidents found that in five cases a lack of needed functions in the overall I&C architecture, and in ten cases inadequate characteristics of I&C functions, contributed to the accidents [1].

For software, the situation is thought to be somewhat worse. It is difficult to understand the performance of software in every possible system state. Thus, it is thought that verification and validation coverage for software designs will be less complete than that which can be provided for hardware. Reference [21] determined that the cost of finding and deleting software defects increases rapidly when attempts are made to reduce defect density below one defect per thousand lines of source code.

5.2.3.2. Surveillance

Surveillance testing and equipment monitoring has been one of the main means of detecting incipient CCF during the last 50 or more years. This testing is mainly directed at finding single failures and the testing is scheduled with the intent to find failures before they occur in redundant systems. It is important to note that as long as the practice continues, human surveillance and testing of equipment provides means for detecting deviations from normal operation that are diverse to features in the electronic systems.

While this testing focuses on random failures, the method has succeeded in detecting potential or actual common cause faults before a failure to respond to demands could result in the occurrence of CCF. The issues affecting HFA relays and DB–50 reactor trip breakers described in Refs [19] and [20], respectively, were identified in this way. A 2007 study of operating experience with digital core protection calculators [22] identified 26 events involving actual or potential CCF over 145 reactor-years. Twenty-three of these events resulted from errors made by instrument technicians, two events resulted from the equipment vendor supplying incorrect data and one from an error in processing logic.

5.2.3.3. Diversity

Digital I&C systems share more data transmission functions and more process equipment than their analogue counterparts. Consequently, different I&C systems may have similar software and/or hardware components. Therefore, a design error in software or hardware could result in the CCF of two or more systems with the potential of compromising multiple levels of defence in depth. The potential for requirement errors or omissions can also be a significant source of CCF vulnerability. As a consequence, the principle of diversity gains importance. Diversity uses dissimilarities in technology, function, implementation, operation and so forth to diminish the potential for

CCF. Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-1.5 [23], provides more information on this subject.

The IAEA definition of diversity [13] is "The presence of two or more independent (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*." Thus, the purpose of diversity is to provide dissimilar means for accomplishing the same or equivalent function in order to ensure independence and minimize the potential for CCF vulnerability.

5.2.3.4. General benefits of diversity

The primary objective of diversity is to minimize the potential for CCF vulnerabilities between levels of defence in depth and/or among systems or subsystems, thereby contributing to establishing the independence of levels of defence.

Some benefits and characteristics of diversity are given in the following:

— Diversity is a means of reducing vulnerability to CCF resulting from errors in requirements, design, manufacturing or maintenance, and of including conservatism to compensate for the difficulty of demonstrating the specified level of reliability.
— Diverse digital or non-digital systems (or indeed manual action if sufficient time and information are available to operators) can compensate for software design errors that should otherwise be considered as a credible source of CCF.
— Diversity is complementary to the defence in depth principle, and defences at different levels of depth may also be diverse from one another.
— Diversity can be used to address identified digital CCF vulnerabilities. Justification of the use of particular diversity attributes is generally required to take credit for the mitigation of such vulnerabilities.

5.2.3.5. Possible drawbacks to be considered in the I&C design

The introduction and potential overuse of diversity can have disadvantages (IEC 60880, annex G.6 [24]). These include greater complexity in the overall I&C architecture, more complex specifications and design, increased space and environmental control requirements, more complicated maintenance demands, and increased costs. These could also result in an increased risk of complex, unanticipated failure scenarios (e.g. spurious actuations leading to unanalysed conditions).

5.2.3.6. Approaches to diversity

There are several forms of diversity that can be applied to differentiate between functions, systems, and components. These generally correspond to physical, functional, and design characteristics. Various diversity types have been defined in the nuclear power industry. IEC 62340 [25], NUREG/CR-6303 [26] and NUREG/CR-7007 [27] provide information on different types of diversity and their potential effectiveness in addressing CCF. Additional information on CCF and mitigation practices is given in Ref. [23].

A number of different types of diversities can be considered either individually or in combination as listed in SSG–39, para. 6.60 [2]:

"— Design diversity: Achieved by the use of different design approaches to solve the same problem or a similar problem.
— Signal diversity: Achieved by systems in which a safety action may be initiated based upon the value of different plant parameters.
— Equipment diversity: Achieved by hardware that employs different technology (e.g. analogue equipment versus digital equipment, solid state equipment versus electromagnetic equipment, or computer based equipment versus equipment based on field programmable gate arrays).
— Functional diversity: Achieved by systems that take different actions to achieve the same safety outcome.

— Diversity in the development process: Achieved by using different design organizations, different management teams, different design and development teams, and different implementation and testing teams.
— Logic diversity: Achieved by use of different software or hardware description languages, different algorithms, different timings of logical functions and different sequencing of logical functions."

Generally, diversity is applied either internally within a system (e.g. by using functionally and/or technologically diverse subsystems) or in separate systems (e.g. by using a diverse actuation system). In many Member States, the diverse or different function may be performed by a system at a lower classification as long as it is of sufficient quality to perform the necessary function under the associated event conditions.

5.2.3.7. Addressing single point vulnerabilities

A single point vulnerability is a single component or subsystem, the failure of which could result in the failure of multiple systems.

When designing an overall I&C architecture, it is generally preferable to avoid single point vulnerabilities that could affect systems belonging to different levels of defence in depth. When a single point vulnerability needs to be introduced, it is a good practice to provide a justification of why it is necessary or beneficial, and a justification of why it will not lead to unacceptable consequences in the plant (e.g. provision of adequate preventive measures ensuring that the single point vulnerability will not fail in a mode or at times that could lead to dangerous CCF, or provision of adequate mitigation measures should that CCF occur).

5.3. INDIVIDUAL I&C SYSTEMS

5.3.1. Single failure criterion

Requirement 25 of SSR-2/1 (Rev. 1) [4] states that "**The single failure criterion shall be applied to each safety group incorporated in the plant design**." Based on the IAEA definitions:

— A 'safety group' is "The assembly of equipment designated to perform all actions required for a particular *initiating* event to ensure that the *limits* specified in the *design basis* for *anticipated operational occurrences* and *design basis accidents* are not exceeded" [13].
— The SFC is "a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure" (from footnote 17 to para. 5.39 of Ref. [4]). To ensure that the SFC is met, usually two or more independent (redundant) systems or trains are provided by design to achieve the same safety function.
— A 'single failure' is "a *failure* which results in the loss of capability of a single *system* or *component* to perform its intended *safety function(s)*, and any consequential *failure(s)* which result from it" [13].

The application of the SFC can be extended so that the safety system or safety group still satisfies the SFC when one of its elements is taken out for service or maintenance. In practice, the SFC requires not only redundancy, but also the independence of the redundant elements.

The measures ensuring the independence of redundant elements and those ensuring the independence of the levels of defence in depth share a number of common principles: physical separation, electrical isolation, functional independence, independence from errors in data communication and independence of support systems. Thus, when designing an overall I&C architecture, these two sets of measures are often considered together in order to avoid unnecessary complexity.

5.3.2. Permissives and bypasses

Permissives and bypasses may be required for various purposes and their consideration may impact on the overall I&C architecture as well as on the design of individual I&C systems. Some examples of permissives and bypasses are included in Sections 5.3.2.1 and 5.3.2.2.

5.3.2.1. Testing and maintenance

Permissives associated with the testing and maintenance of redundant safety systems may perform a number of functions. They may:

— Force the redundant element under maintenance to a known state (or at least in respect of how it appears within the I&C systems) such that the I&C system is temporarily reconfigured (e.g. from a 2 out of 4 vote to a 2 out of 3 vote);
— Provide indication that the unit is under test;
— Prevent more than one redundant element from undergoing maintenance simultaneously.

However, it is also possible that such arrangements may need to consider multiple systems within the architecture. For example, it may be desired to engineer a permissive such that the protection system and its diverse backup cannot undergo maintenance at the same time.

5.3.2.2. Operation

Bypasses may be required dependent on the plant's mode of operation. A typical example is during startup when the reactor increases in power and the operator needs to increase from one power range set point to a higher one. The design of this bypass is potentially an architecture issue for two reasons. Firstly, it may be necessary to change the set points in both the protection system and in any diverse backup, and to all redundant channels within those systems, while adequate independence needs to be maintained. Secondly, the means by which this is achieved involves the operator, and so a decision must be taken on the HSI to be used. As this permissive factor affects protection system functionality, it may suggest that dedicated controls at the highest classification are used. Alternatively, this is just one step in a series of operations being taken by the operator during power raise, and it may be appropriate to allow the operator to take this action from the normal operational stations. Such an approach would avoid the need for the operator to move away from the physical location, from the context of the step and from the displays of other related information, but may mean the transfer of the permissive from a lower classified system to the protection system. These sorts of design trade-off issues affecting different aspects of safety need to be considered in an integrated fashion in conjunction with other design disciplines.

5.3.3. Protection against spurious actuations caused by random failures

The term 'spurious actuation' refers to erroneous control caused by active I&C failures (whereas passive I&C failures would lead to a loss of the desired I&C function). Active failures are further subdivided into random failures and systematic failures as follows:

— Random failures are a consequence of physical or chemical effects, which may occur at any time. A good description of the probability of the occurrence of random faults can be given using statistics (failure rate). Increased failure rates may be the consequence of systematic faults in hardware design or manufacture, if these occur without temporal correlation, for example, as a consequence of premature ageing (see IEC 62340 [25]).
— Systematic failures are, in a deterministic way, related to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors (see IEC 62340 [25]).

Redundancy can be used to provide some level of defence against spurious actuations caused by random failures.

5.3.4. Independence of I&C system segments

Digital technologies have many benefits. However, the concentration of many functions in the same I&C systems and the increased level of data communication mean that a failure could affect a large number of I&C functions and could have adverse effects on the performance and availability of the plant. Thus, it is generally

beneficial to organize such I&C systems into subsystems (often called segments) that are reasonably independent from one another, so that the failure of one segment has limited and acceptable effects on plant operation, and is not likely to propagate to other segments. For example, segmentation may be used:

— To separate process control functions from those that may play a role in detecting or mitigating the failure of those controls;
— To ensure that redundant process trains are controlled by separate segments;
— To separate the control functions assumed to be so by the probabilistic safety assessment;
— To facilitate construction and maintenance activities.

The level of independence for such segments is in general not as high as that necessary for the levels of defence in depth or for the SFC. However, the measures taken for the latter (e.g. independent support systems and separate rooms) may be exploited for the benefit of the former.

Segmentation is not only a control system issue to limit the scope of failure. It is also widely applied in relation to functional diversity within safety systems. For example, where plant events can be detected using two different process parameters (e.g. temperature and pressure), then it is likely to be beneficial to partition these two parameters in different units so that a single failure cannot affect both. Similarly, if diverse functions (e.g. two different means of heat removal) are used to respond to an event then these might also be partitioned.

For adequate segmentation, it is necessary to have an appropriate set of I&C functions, and I&C architects can inform the other plant designers of their needs in this respect.

5.4. FUNCTIONAL SPECIFICATION FOR I&C AND SAFETY CLASSIFICATION OF I&C SYSTEMS

The goal of the categorization of functions and classification of equipment and systems is to facilitate a graded approach for the technical and quality requirements of functions and systems. Functions belonging to a higher safety category and systems belonging to a higher safety class will have stricter requirements than those that belong to lower safety categories or classes.

5.4.1. Categorization of functions

The I&C functions required for meeting safety goals and functions in all plant states are categorized on the basis of their safety significance. This is detailed in Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG–30 [28]. For the purposes of this publication, the safety significance of each function can be described as being determined by:

— The severity of consequences (high, medium and low), if the function were not performed when challenged;
— The frequency of occurrence of the PIEs that call for performing the given function;
— The purpose of activating the given function (to reach a controlled state or a safe state).

In SSG-30 [28], the categorization of functions is based on the following three safety categories:

— Safety category 1:
  • Any function that is required to reach the controlled state, and whose failure, when challenged, would result in consequences of ‘high’ severity.
— Safety category 2:
  • The same as above, but with consequences of ‘medium’ severity.
  • Or any function that is required to reach and maintain a long term safe state and whose failure, when challenged, would result in consequences of ‘high’ severity.
  • Or any function that is designed to provide a backup of a function categorized in safety category 1.
— Safety category 3:
  • There are five possibilities listed in this category (see SSG-30 [28]).

5.4.2. Classification of I&C systems

Once the safety categorization of I&C functions has been completed, the I&C systems performing these functions should be assigned to a safety class.

All I&C systems required to perform a function that is safety categorized should be identified and classified according to their safety significance following a process described in SSR-2/1 (Rev. 1) [4].

The safety classes of I&C systems are defined as:

— Safety Class 1: Any I&C system, the failure of which would lead to consequences of 'high' severity;
— Safety Class 2: Any I&C system, the failure of which would lead to consequences of 'medium' severity;
— Safety Class 3: Any I&C system, the failure of which would lead to consequences of 'low' severity.

By assigning each I&C system to a safety class, a set of engineering, design and manufacturing rules can be identified and applied to the I&C systems to achieve the appropriate quality and reliability. Safety classification is an iterative engineering design task. Guidance on its rules and processes is given in Refs [28] and [29].

Owing to differences in safety categorization and classification schemes, Member States may introduce different graded requirements on assigning I&C functions and systems to safety categories and classes.

If an I&C system or equipment contributes to the performance of several functions of different categories, it is assigned to the class corresponding to the highest of these categories (i.e. the one requiring the most conservative engineering design rules).

The safety class of an actuator is derived from the highest safety category of the function(s) it performs. As a consequence, commands to actuators from various I&C functions have to go through a priority logic such that the lower category function does not hinder the performance of the higher category function.

5.4.3. Functional specification for I&C

The main duty of I&C systems is monitoring and controlling the nuclear and other physical processes (e.g. thermohydraulic or electric processes) of the nuclear power plant. I&C designers are usually not experts in neutron physics and physics; therefore the most important inputs for the work of designing I&C systems are the functional requirements that are formulated by safety, process and equipment engineers. The communication between designers of different disciplines needs to be initiated as early as possible in the design process, and it needs to be unambiguous. However, experience shows that this is a significant issue. To limit the potential for misunderstandings, the following are needed from safety, process and equipment engineering:

— Identification of each I&C control function according to the objective of the process tasks with a unique identifier to facilitate formal design and configuration management tasks, in particular, identification of the role, if any, of each I&C function with respect to the related PIEs;
— Assignment of each I&C control function to a safety category according to the safety significance of the associated process task;
— Defence in depth concept of the plant, and assignment of each I&C function to the appropriate level of defence in depth;
— Segregation requirements between I&C control functions;
— Explicit requirements of functional diversity for the PIEs;
— Performance requirements, such as response times, accuracy, etc. for each I&C control function.
— Inputs (sensors, outputs of other functions) and outputs;
— Definition of fail-safe state or position for each output, which needs to be set in case of a detected failure;
— Specification of required operator intervention in relation to the I&C control function, for normal, abnormal and accident conditions, in such a way that the operating personnel can perform their task;
— In addition to human language description, a multilevel, hierarchical and well-structured formal language (software and diagrams) description to avoid misunderstanding due to usage of ambiguous human language;
— Identification and grading of information needed for performing the operators' task and for monitoring the automatic functions (including group alarms, combined alarms and alarm classes);

— Accuracy requirements for setting up set points and thresholds (including hysteresis) and displaying analogue values;
— Reliability targets from safety and process engineering;
— Wherever applicable, a rationale needs to accompany the requirements to establish a clear link to the underlying basis.

It is essential that these inputs to I&C design meet certain criteria. In particular, the inputs of a function determine intrinsic dependencies: if a function in one defence in depth level needs an input that is the output of another function in another level, then there could be a functional dependency between these two levels. Similarly, if a function of a certain safety category needs an input that is the output of another function of a different safety category, then there could be a functional dependency between these two functions. In addition to I&C functions defined by process engineering, further functions that have features specific to the I&C discipline will be defined by the I&C engineers. Examples of these functions are testing, diagnostics, monitoring, parameter adjustment and other maintenance supporting I&C functions. These I&C specific functions are specified in the same way as safety and process functions, but their significance to safety is lower than those of I&C control functions.

Functional specifications and requirements, especially those pertinent to achievement of safety functions, could be managed through databases. This improves their visibility to the involved parties, allows for more robust configuration management and serves to provide bidirectional traceability of the specifications to the underlying design bases.

5.5. COMPUTER SECURITY

Cyberattacks on nuclear power plants might cause the failure or mal-operation of I&C systems, which can pose a significant hazard to nuclear power plants. Attacks on any level of defence in depth might cause conditions that are beyond design basis assumptions. Furthermore, multiple levels of defence in depth may be attacked at the same time. The overall I&C architecture needs to specify strategies for preventing, detecting and mitigating the effects of such attacks. Several different approaches can be applied as part of the overall I&C architecture.

There is a significant number of computer security guidelines in practice today, but only a few of them are applicable to I&C architecture development, while others are more applicable to policy or specific technology architecture work. Those principles relevant to the overall I&C architecture are the focus of this publication.

5.5.1. Conceptual security models

Throughout this publication, reference is made to a conceptual security model, intended to be used as an input to various steps of the architecture development process. This model defines various computer security zones, which are analogous to the security levels defined in IAEA Nuclear Security Series No. 17 [8] and are further detailed in Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T [30]. The model also defines how those zones are related, and provides guidelines to classify control functions and information assigned to defined zones.

The I&C system data confidentiality is not necessarily unimportant, but it is not *as* important as data integrity. There needs to be confidence in both system commands and state information flowing throughout the system. From an operational perspective, it is much less important that this data be kept confidential. In line with this, conceptual security plans for I&C systems could place more emphasis on data integrity than confidentiality.

5.5.2. Limitation of the extent to which I&C systems can control plant functions

The design of nuclear power plants includes provisions to limit the extent to which I&C systems can control plant systems and critical parameters. For example:

— Control rod drive systems prevent simultaneous movement of multiple control rod banks and mechanical speed limitations on control rod drives restrict the rate at which the rod drive system can insert reactivity.

— Mechanical safety valves prevent I&C systems from increasing the reactor coolant system pressure above safe limits during power operation.
— Physical lockout of power to motor operated valves prevents control systems from changing the valve state without operator intervention.

Currently, these features are intended to prevent I&C system, subsystem or component failures that could lead to accident conditions, but in some cases these features may also protect against or act to limit the consequences of cyberattack. These features generally exist within the non-I&C portions of the plant and it is necessary for the I&C system design engineers to work with plant design engineers to limit the possible consequences of I&C system mal-operation. Plant features that take credit for physics, mechanical components, mechanical system characteristics, non-digital I&C systems and equipment, or strong administrative controls can limit the consequences that can be caused by cyberattack and can be a very robust form of computer security.

It is extremely important that during a cyberattack: (i) operators have means to know that such an attack is under way; and (ii) operators have a minimum subset of trustworthy plant data. Consequently, it may be prudent to consider whether an essential subset of I&C systems, subsystems or components, needed to maintain reactor safety and to execute critical safety functions, might be implemented in a non-programmable technology.

5.5.3. Computer security protection features as part of the overall I&C architecture

Many features introduced into the overall I&C architecture for safety reasons can also provide protection against cyberattack. For example, SSG–39 [2] contains the following guidance:

— “The effects of a failure of an automatic control system [or multiple spurious actions of controls systems) should not create a condition that exceeds the acceptance criteria or assumptions established for design basis accidents” (para. 7.14).
— “Only predefined messages should be processed by a receiving safety system” (para. 7.93).
— All data connections for systems and components should be placed within enclosures for which both access to the enclosure and access to the inside of the enclosure are controlled (para. 7.112) and “Unused data connections should be disabled” (para. 7.114).
— “Indication of the states of operational bypasses should be provided in the control room” (para. 7.37).

The introduction of additional computer security measures into I&C systems should respect the guidance in SSG–39 [2] and IAEA Nuclear Security Series No. 33–T [30], which states that neither operation nor failure of any computer security function should adversely affect the ability of a system to perform its safety function.

5.5.4. Protection against cyber threat

Although the requirements and design of the computer security defensive architecture, and that of the corresponding zoning schemes and security boundaries, are outside the scope of this publication, it is an important consideration for the development of the overall I&C architecture.

The overall I&C architecture of the nuclear power plant needs to be aligned with the computer security defensive architecture. The I&C systems important to safety, and their interconnections, need to be designed in such a way that there is adequate protection from cyberattacks in order to maintain confidentiality, integrity and availability. Defensive features are incorporated to provide a secure operational environment and to protect against cyberattacks.

Computer security imposes its own organizational ontology, frequently based on risks, such as those described in Refs [8] and [30], on the equipment to be used based on the security significance of the functions they implement and based on their vulnerability to cyber threats. This ontology imposes requirements and constraints on the choice of platforms (and their development environments) used to realize the overall I&C architecture. These requirements and constraints need to be documented early in the project phase so that they can be considered while developing the technical specifications and while carrying out the technical evaluation of the I&C platforms being considered.

Some examples of controls that may be considered requirements for the individual I&C systems may include access control and account management, event monitoring to support the investigation of security incidents, and communication protection. Access control may include restrictions on wireless and portable device access. Boundary protection, especially between different defence in depth levels within the overall I&C architecture, may be by physical enforcement of one-way communication from a higher to lower level. Provisions may be made to ensure that unauthorized information flows are detected, deterred and prevented.

Similarly, the development environment for digital I&C systems may have suitable measures for preventing the intentional or unintentional intrusion or corruption of the software or data, the introduction of malicious code, incorrect connection to external networks and hacking attacks. Requirements for teams to work together to develop system software, for example, is one way to both increase the overall quality of the developed software and to ensure that no single engineer can inject flaws, backdoors or other malicious code into software deployed into high consequence environments. Likewise, requiring technicians to work together when maintaining critical systems can enforce correct procedural compliance and lead to higher quality outcomes.

The implementation of security controls or functions is carried out in a manner such that implementation does not adversely impact the performance, response time or effectiveness of the safety function. Where security control is employed as a safety control or safety HSI, it is employed in such a way that the security controls do not adversely affect the ability of the system to perform its safety functions or that of the operator to control the plant. Security controls within an I&C system important to safety are developed and qualified to the same level of qualification as the system in which these security controls reside.

In general, the overall I&C architecture ensures that the systems that have the highest importance to safety are segregated or independent from the ones that are of less importance to safety. The design provisions that address this are generally also helpful in meeting the security requirements. However, at times, the security and safety requirements are different and can be conflicting if not carefully implemented. To the extent possible, the security and safety requirements should be addressed so that they do not compromise one another — for example, the complexity introduced by security controls may have the potential to cause degradation in the I&C system response time.

The failure modes of computer security features and the effects of these failure modes on I&C functions need to be identified, documented and considered as part of the I&C system hazard analyses. The overall architecture and its building blocks have provisions for periodic and post-maintenance verification, to confirm that the security features are properly configured and operating.

Some computer security features may be inappropriate for incorporation directly into systems, subsystems and/or components that implement plant I&C functions. For example, access logging within the plant I&C system may have undesired effects on the plant functions as the size of the logged data file grows. It may be more appropriate to implement some of the computer security functions in dedicated systems that are connected to, but isolated from, the I&C systems used for plant control and protection.

5.6. I&C FAILURE POSTULATES

Most standards organizations and regulators require hazard analyses with the intention of identifying failure postulates (i.e. failures not practically eliminated that might compromise the overall safety of the plant) and to verify that the proposed design solutions are sufficient to cope with them. In particular, SSG–39 [2] para. 2.56, recommends that “For the overall I&C architecture, a hazard analysis should be performed to identify conditions that might compromise the defence in depth or the strategy for diversity of the plant design.” It also provides a first rough overview of the core areas to be analysed (see also Ref. [31]). SSG–39 [2], para 2.61, points out that the requested analysis “should be updated at every phase of the development life cycle, including … the design of the overall I&C architecture…”. The results of the analysis can lead to measures being “taken to eliminate, avoid or mitigate the consequences of identified hazards that could degrade the performance of system functions” (para. 2.63, Ref. [2]).

The prerequisite for a hazard analysis is the identification of the scope of failure postulates and the analysis of the resulting events. The generic list of PIEs to be considered is quoted in the preliminary safety analysis report. These events are focused on the overall plant and typically do not consider I&C failure postulates, though there may be exceptions. Even when it is not required for the preliminary safety analysis report, it is a good practice

to synchronize the list of I&C failure postulates to be considered between the stakeholders at an early stage of the project.

The effectiveness of the different barriers is evaluated with respect to each I&C failure postulate. In the evaluation, it may be helpful to consider the evolution chronology in Fig. 9 and take into account possible escalation and dependencies. In the end of this process, evidence is provided that for each failure postulate and barrier, the design provisions realized either by I&C (overall I&C architecture, I&C systems, I&C components) or by other disciplines (civil, electrical, HVAC, etc.) are appropriate.

For each I&C failure postulate, the likelihood and the possible consequences need to be considered. Unrealistic scenarios and failure combinations could be counterproductive, as the introduction of the corresponding design measures may result in a significant increase of complexity (in design, operation and maintenance) and may increase the potential for spurious actuations (which may have a non-negligible adverse effect on safety).

Lessons learned from operational experience [32], including from industrial sectors other than nuclear, could be assessed from the specific viewpoint of the nuclear industry. The focus would be on the specific priorities and objectives in each particular context, and the effectiveness of particular digital design features and methods in preventing certain types of faults and failures.

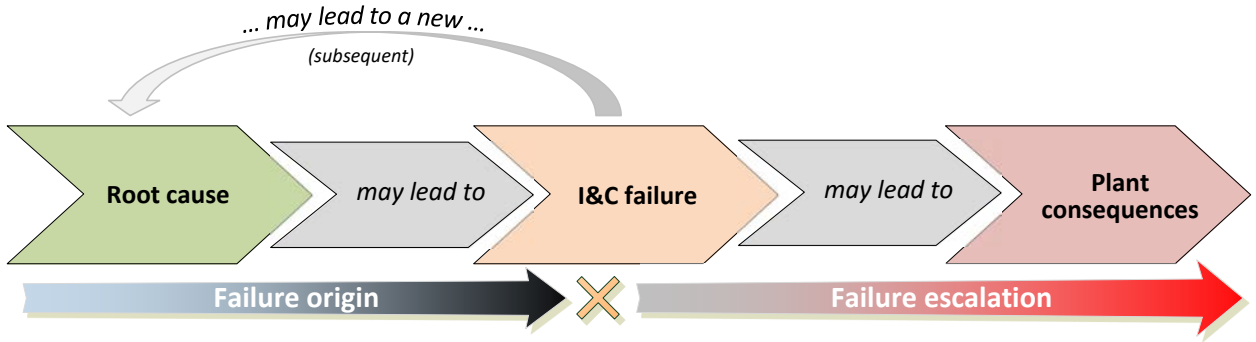


FIG. 9. I&C event evolution (generic chronology).

5.7. DEDICATED I&C SYSTEMS AND DEVICES

Some plant systems or components may be provided with their own dedicated I&C systems and devices. These may or may not be interconnected with I&C systems and devices that are parts of the plant's overall I&C architecture. In such cases, and also when they play a role in anticipated operational occurrences, design basis accidents or design extension conditions, it is good practice to include them in the overall I&C architecture. Their respective importance to safety and computer security needs to be determined, and they need to be allocated to specific levels of defence in depth and security zones.

5.8. DYNAMIC ASPECTS OF OVERALL I&C ARCHITECTURES

At particular times, temporary equipment might be connected to the overall I&C architecture or to individual I&C systems, and then disconnected when no longer necessary. Also, the configuration of a given I&C system or component may evolve in time. This may be done for many different purposes, such as:

— Maintenance, periodic testing and/or calibration of particular systems and components;
— Downloading of new process parameter values or new software versions;
— Addressing the specific functional needs of plant outages;
— Addressing the specific functional needs of particular incident or accident situations.

Such temporary changes need to be clearly identified, and their effects need to be evaluated from operational, safety and computer security standpoints. Measures need to be taken to prevent or signal unauthorized, malicious or inadvertent changes, and to ensure that changes that are actually performed do not compromise the following:

— The independence of the levels of defence in depth designed in the overall I&C architecture. For example, a piece of temporary equipment might need to be assigned to a level of defence in depth so that it cannot adversely affect the other levels in case of malfunction.
— The correct functioning and dependability of the permanent I&C systems and equipment. For example, the qualification and safety assessment of the permanent I&C systems and equipment need to consider their possible configurations and to take into account the effects of the connection and disconnection, and of the presence and absence, of temporary equipment. A piece of temporary equipment may also be assigned a safety class.
— The computer security of the overall I&C architecture and of its constituent systems. For example, a piece of temporary equipment might need to be assigned to a security zone so that it is adequately protected against malicious attacks, in a manner commensurate with the security degree and security zone of the I&C systems to which it will be connected and with which it will interact, and with the measures taken to verify their actions and/or outputs.

5.9. FEATURES SUPPORTING TESTING AND DIAGNOSTICS

5.9.1. Verification and validation testing

The systems that compose the overall I&C architecture need to be rigorously verified and validated, first separately on a system by system basis, and then as an integrated whole as defined by the overall I&C architecture. Among the various techniques that may be applied, testing plays an important role. Due to the large number of I&C functions implemented by the individual I&C systems, and also due to the need to retest the systems after they are modified, it is often worthwhile to consider using dedicated test environments. Such environments are designed to facilitate running a large number of test cases in a way that is reproducible and supports automatic evaluation and documentation. These environments may operate in an open loop (i.e. without the feedback of a process simulator) or in a closed loop, using a suitable process simulator.

It might be necessary to perform design modifications during the operational lifetime of an I&C system important to safety. It is often a good practice to have an off-line (i.e. not connected in any way to the plant process, systems and equipment) test and maintenance facility that is capable of performing the following tasks:

— Testing I&C functionality;
— Observing and possibly recording the behaviour of particular parts of the I&C system;
— Training for the I&C operations and maintenance personnel;
— Testing the spare modules and troubleshooting;
— Testing any algorithm and HSI modifications;
— Computer security vulnerability testing;
— Cooperation and real time operation with process models, in the framework of the test environment.

This test and maintenance facility does not necessarily need to be identical to the I&C system, but it needs to be demonstrably representative.

5.9.2. Periodic testing, monitoring and diagnostics

In addition to the self-monitoring that is continuously active during an I&C system's normal operation, the liveliness of the system could be monitored by other systems or devices, preferably (but not necessarily) in the same defence in depth level. Also, the monitoring of data communications by pure observers (i.e. systems or devices that can observe the data exchanges but cannot interfere) may provide useful information to detect abnormal situations and for diagnostics.

Even though such monitoring may identify some categories of problems more rapidly, it does not eliminate the need for channel checks and surveillance testing (both those required by operating limits and conditions, and those conducted just as a matter of good practice) by operators and maintenance technicians. Supporting features may be provided by temporarily connected service and maintenance units. Also, care needs to be taken to avoid spurious diagnostics due either to poor design or to poor computer security.

5.10. ARCHITECTURE DESIGN TO FACILITATE FUTURE UPGRADES AND MODERNIZATION

The significant difference in the lifetime of a nuclear power plant and its I&C systems makes it necessary to retrofit (form, fit and function modules replacement), upgrade (I&C system replacement with limited changes in the overall I&C architecture) or modernize (significant changes in the overall I&C architecture) the I&C during the operational time of the plant. Most nuclear power plant operators have collected some experience with plant lifetime extension and I&C systems modernization. Several publications contain information on when and how the modernizations need to be implemented. Examples are:

— IAEA-TECDOC-1389, Managing Modernization of Nuclear Power Plant Instrumentation and Control Systems [33];
— IAEA Nuclear Energy Series No. NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants [34].

The accumulated experience also identifies the problems that have caused difficulties in past projects. It provides an input for architecture designers to facilitate I&C system retrofits, upgrades and modernizations. The I&C architects may consider the following lessons learned:

— The architect needs to elaborate a lifetime management procedure for the I&C systems and acquire supporting tools for implementing the procedure. This procedure may include continuous condition monitoring and preventive measures such as I&C system retrofits, upgrades or modernizations. The procedure may also include a renovation strategy, for example:
  • Replacement of failed modules only;
  • System upgrades that replace obsolete components with newer versions that meet the form, fit and function requirements at the first and the third quarter of the planned lifetime of the plant;
  • Modernization at the half lifetime of the plant.
— The architecture needs to be modular with standard and/or well-documented interfaces to facilitate module or I&C system replacements. Partitioning of the overall I&C architecture helps to avoid unnecessary complexity and interactions between individual I&C systems, and hence promotes ease of modification.
— Poor documentation leads to a large effort and reverse engineering when a module or an I&C system needs to be replaced. A problem often encountered when modernizing, upgrading or modifying systems is that the rationale for the original design decisions is no longer available at the time when the change is to be made. This can cause misunderstandings or misinterpretations and hence can lead to design errors being made during the change process. Consequently, an important objective to support future maintainability and sustainability is not only for the design information to be retained, but also the rationale and justification for the decisions taken during the design and for any subrequirements arising as a consequence of those decisions. The overall I&C architecture designers need to provide high quality documentation that includes the background analysis used for the design. It is to be noted that good documentation will disappear if a strict configuration management is not ensured.
— It is also necessary to keep track of any changes during the plant's lifetime (e.g. the addition of equipment that increases electromagnetic radiation and the risk of interference) in order to keep the design information up-to-date when modernizing the I&C systems or components.
— Longer outage time may be needed for comprehensive renovation. The architecture designer could provide sufficient possibilities to preinstall a new I&C system during plant operation in order to reduce both the installation and the commissioning time. (This comprehensive renovation can be harmonized with other large mechanical maintenance or renovation tasks.)

— Untidy cabling on overloaded cableways can cause extra work, whereas transparent cabling installed on easy to access cable ways could be designed to facilitate partial replacements in case of need.
— During the long operational time of the plant, functional extensions will probably be needed. The architecture needs to be flexible enough. The I&C architect could include sufficient spare resources to ease future functional extensions, taking into account the spare capacity often required during commissioning for I&C system tuning.
— It cannot be excluded that after decades of operation, when comprehensive renewal of the I&C systems is due, changes to the architecture will also be necessary owing to new requirements. The architect could provide flexibility, spare capacity, empty places for cabinets and empty places and penetrations for new cables to ease such possible modifications.

5.11. NON-FUNCTIONAL CONSIDERATIONS FOR I&C ARCHITECTURAL CHOICES

A number of non-functional objectives and considerations may need to be taken into account in the design of the overall I&C architecture. These include:

— Elimination of single point vulnerabilities that have caused system failure and/or plant shutdown;
— Obsolescence of existing equipment and lack of spare parts;
— Reduction of operations and maintenance costs (e.g. reducing necessary human resources or the need to work in a contaminated environment);
— Standardization of vendor component and platform across a fleet of plants;
— On-line maintenance versus outage maintenance;
— Installation to support plant operations (e.g. during a specific refuelling outage or per regulatory requirement);
— Timeliness of regulatory review;
— Existing plant system and regulatory requirements.

Other examples of non-functional considerations that can impact overall I&C architecture are given in Section 5.11.1.

5.11.1. Physical constraints

The physical constraints of the existing analogue architecture will often determine the physical layout of a proposed new digital system. If cost is a primary project driver, then a system that uses the existing footprint may be the better choice since it will cost less to install if existing cabinets, field wiring, power, and heating or ventilation are reused. However, using the existing cabinets can complicate installation since the overall analogue I&C architecture may be significantly different from the new digital architecture. It may require extensive rewiring of inputs to support functional partitioning and future maintenance. If the installation window is small, this may be an issue.

Use of remote input/output and fieldbus techniques may eliminate the need for extensive rewiring and limit the number of digital components to later be maintained. However, system design requirements may prohibit critical input parameters from traversing the network (i.e. require hardwiring or locating processors in the file near the input/output).

The number of sensors in the field for retrofits can be retained or changed to address shortcomings or vulnerabilities in the new digital system. More sensors may be desired to increase the reliability of the controls or reduce the need for ongoing maintenance; however, these additional sensors will add additional costs and complexity and must be weighed against the overall goals of the new system.

5.11.2. Impact of life cycle considerations

5.11.2.1. Industrial non-nuclear platform versus nuclear specific platform

Selection of an industrial non-nuclear specific platform will provide a platform with extensive operating experience and flexibility. It will support the latest standards and may better meet the operational goals of efficient process control and increased on-line maintenance. It may also be less expensive to purchase and install, but the ongoing life cycle maintenance and more rapid obsolescence of this platform may detract from these savings over the life of the platform. In contrast, a platform developed specifically for the nuclear industry will often be costlier and have less flexibility or capabilities. However, there may be longer term savings in fewer periodic updates or software changes and a longer term commitment of support from the original equipment manufacturer.

5.11.2.2. Operational considerations

Every decision could be graded against how it changes the life cycle cost and impacts future operational considerations (e.g. plant life extension, changing modes of operation from baseload to load follow, new regulatory requirements and overall security posture). Some plants will be operating in competitive markets where life cycle costs are a primary driver for the viability of the plant. Other plants may operate in a more regulated market where a reasonable return is guaranteed. The total life cycle costs of the overall I&C architecture need to be considered with respect to the operational goals of the plant. Implementing changes in the I&C to allow for reduced staffing, reduced maintenance and novel operating modes need to include the costs of the I&C life cycle along with the cost associated with the implementation of the proposed changes. A more expensive and less capable system that has lower ongoing maintenance costs may make more sense in the long run. Life cycle cost includes the cost of software upgrades, patching, purchase and storage of spare parts, ease of maintainability, training, plant reliability impacts, and support for existing and anticipated operational modes.

5.11.2.3. Plant and fleet level standardization

Plant and fleet level standardization can have significant economic benefits by reducing overall life cycle costs via fewer spare part needs, less training requirements and standardized maintenance routines. However, it may complicate licensing if it is perceived to reduce diversity between protection and control. Additional costs in assuring independence may erode all the savings from standardization. There may be limits on the level of standardization between the levels of defence, particularly between the protection and plant controls systems. Fleet level standardization can help in this area as the independence and diversity between protection and controls can be maintained and the benefits of standardization can be realized at the fleet level with the overall fleet reduction in spares and expertise. In addition, many ongoing life cycle costs associated with the maintenance of a digital system such as software upgrades, patching and obsolescence prevention measures can be addressed at the fleet level once and the cost shared at the plant level when separately implemented at the sites.

6. CONCLUSIONS

As discussed in this publication, the overall I&C architecture of a nuclear power plant is the organization of the complete set of I&C systems important to safety. The architecture establishes:

— The I&C systems that comprise the overall architecture;
— The organization of these systems using a defence in depth concept;
— The allocation of I&C functions to these systems;
— The interconnections across the I&C systems and the respective interactions allocated and prohibited;
— The design constraints (including prohibited interactions and behaviours) allocated to the overall architecture;
— The definition of the boundaries among the various I&C systems.

Therefore, the overall I&C architecture gives a high level view of the individual I&C systems and how they relate to one another. The primary functions assigned to I&C systems are derived from the plant design basis and consideration of design extension conditions. They involve protection, control and monitoring.

An important requirement from SSR-2/1 (Rev. 1) (Requirement 7, Ref. [4]) is independence among levels of defence in depth, to enable one level of defence to compensate for the failure of another level. The overall I&C architecture and the constituent I&C systems can be characterized in terms of layers of elements from the plant itself to the staff (e.g. operators, engineers, maintenance departments and management) and levels of defence.

Therefore, key principles for an overall I&C architecture of a nuclear power plants considered within this publication include the:

— Grouping of I&C systems into levels of defence in depth such that if a failure occurs in one level, it can be compensated for or corrected by another level or other levels, without causing harm.
— Categorization of I&C functions and classification of I&C systems, which is performed according to their importance to safety.
— Independence among levels of defence in depth and among safety classes, so that:
  (a) An event that adversely affects one level, together with its consequences, does not reduce the effectiveness of the other levels in performing their functions important to safety;
  (b) An event that adversely affects an I&C system, together with its consequences, does not affect the effectiveness of systems that are more important to safety in performing their functions important to safety.
— Establishment of computer security concepts and definition of computer security groupings into zones.
— Integration in, and consistency with, the plant architecture and concepts, in particular for safety (including defence in depth), security and operation, as the implementation of the principles in I&C may place specific constraints on the plant nuclear, mechanical or functional design, and on operation and maintenance planning.
— Elimination of unnecessary complexity and the location of necessary complexity where it can be best controlled.
— Appropriate location and protection of I&C equipment against hazardous environments.

The overall I&C architecture and the constituent I&C systems can be characterized in terms of layers of elements from the plant itself to the human staff (e.g. operators, engineers, maintenance departments, management) and levels of defence. The elementary layers can be grouped as follows:

— Layer 0: Sensors and actuators;
— Layer 1: Field control;
— Layer 2: Process control and protection;
— Layer 3: Supervisory control and information;
— Layer 4: Technical management.

The levels of defence prevent accident progression through the provision of independent systems performing different functions, such that failure at one level does not prevent the other levels from performing their functions. The typical functions performed at each level are as follows:

— Level 1: Plant control under normal conditions;
— Level 2: Monitoring for abnormal conditions and automatic inhibit functions;
— Level 3: Reactor trip and actuation of engineered safety features (e.g. to remove decay heat);
— Level 4: Monitoring and mitigation of severe accidents;
— Level 5: Monitoring of radioactive releases.

The life cycle of the overall I&C architecture can be divided into three major steps:

— Installation of the first I&C;
— I&C modernization and maintenance;
— Decommissioning.

The modernization of I&C in existing power plants results in specific challenges, since only certain parts of the plant are directly concerned. Therefore, the existing overall I&C architecture would not normally be drastically changed. In particular, it is necessary to consider compatibility with the existing infrastructure, the impact of changes on interrelated systems, the impact of installation activities and the potential introduction of new security vulnerability exposure.

For new plant designs, the development of the overall I&C architecture begins as part of the plant's conceptual design. Certain architectural decisions need to be made up front, such as redundancy within safety systems, the degree of separation between those redundancies, between the safety system and control systems, and among systems assigned to different levels of defence.

Extending from the conceptual design phase, the overall I&C architecture will evolve based on ongoing discussions with design teams from other disciplines. As the plant design moves from general ideas to concrete designs, I&C engineers must continually evaluate the implications of decisions taken by design teams from other disciplines on the I&C design. They must also collaborate with these other teams to avoid unnecessary demands being imposed on the I&C design, and communicate to ensure the other teams are aware of inputs and information they should provide to support the ongoing development of the overall I&C architecture.

This publication also provides guidance regarding:

— The organization of the overall I&C architecture design process into successive steps, with feedback from the stakeholders concerned, in order to limit the need for significant architectural changes during detailed design;
— The dedicated I&C systems and devices that are integral parts of particular plant systems or equipment;
— The temporary equipment that might be connected to the overall I&C architecture or to individual I&C systems, and then disconnected when no longer needed;
— The need to adequately support the verification and validation of the integrated set of I&C systems constituting the overall I&C architecture, and the monitoring, testing and maintenance of I&C equipment.

The design of an overall I&C architecture is a difficult and complex task that requires information and is subject to constraints from many different sources. It needs to be considered as an integral part of the plant design and of the operation and maintenance planning. This is because an appropriate solution to an I&C architecture issue will sometimes place constraints on other engineering disciplines. The overall I&C architecture also needs to be extensively documented together with its rationales, so that the I&C can be maintained and upgraded during the lifetime of the plant.

It can be noted that the suggestions in this publication might be considered for adaptation in other nuclear facilities of the fuel cycle in compliance with relevant standards and guidance specific to those facilities.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-1.13, IAEA, Vienna (2015).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[3] 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).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[5] ELECTRIC POWER RESEARCH INSTITUTE, Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments, 3002002953, EPRI, Palo Alto, CA (2014).

[6] AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY OF AUTOMATION, Enterprise-control System Integration, ANSI/ISA-95, ANSI/ISA, New York (2010).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Classification of Instrumentation and Control Functions, IEC Standard 61226, 3rd edn, IEC, Geneva (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[9] BLOOMFIELD, R.E., BISHOP, P.G., JONES, C.C.M., FROOME, P.K.D., Adelard Safety Case Development (ASCAD) Manual (1998), https://www.adelard.com/resources/ascad.html

[10] BLOOMFIELD, R.E., et al., Guidance on Claims, Arguments and Evidence (2017), http://www.ClaimsArgumentsEvidence.org

[11] BISHOP, P.G., BLOOMFIELD, R.E., "A methodology for safety case development", Safety-Critical Systems (Proc. 6th Symp. Birmingham, 1998) (REDMILL, F., ANDERSON, T., Eds), Springer, London (1998).

[12] TOULMIN, S.E., The Uses of Argument, Cambridge University Press, Cambridge (1958).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (in press).

[14] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, Safety of new NPP designs, Study by Reactor Harmonization Working Group RHWG, WENRA (2013).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Criteria for Diverse Actuation Systems for Nuclear Power Plants, IAEA-TECDOC-1848, IAEA, Vienna (2018).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Monitoring Systems for Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.16, IAEA, Vienna (2015).

[17] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants: Instrumentation and Control Systems Important to Safety, General Requirements for Systems, IEC Standard 61513, IEC, Geneva (2011).

[18] ELECTRIC POWER RESEARCH INSTITUTE, Severe Nuclear Accidents: Lessons Learned for Instrumentation, Control and Human Factors, 3002005385, EPRI, Palo Alto, CA (2015).

[19] NUCLEAR REGULATORY COMMISSION, Failures of General Electric Type HFA Relays in Use in Class 1E Safety Systems, Bulletin 84-02, Office of Inspection and Enforcement, Washington, DC (1984).

[20] NUCLEAR REGULATORY COMMISSION, Failure of Reactor Trip Breakers (Westinghouse DB–50) to Open on Automatic Trip Signal, Bulletin 83-01, Office of Inspection and Enforcement, Washington, DC (1983).

[21] KRASNER, H., Using the Cost of Quality Approach for Software, Crosstalk **Nov.** (1998) 6–11.

[22] BICKEL, J., "Risk implications of digital RPS operating experience", paper presented at IAEA Techn. Mtng on Common-cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants, Vienna, 2007.

[23] 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).

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

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

[26] NUCLEAR REGULATORY COMMISSION, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, Office of Nuclear Regulatory Research, Washington, DC (1994).

[27] NUCLEAR REGULATORY COMMISSION, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, NUREG/CR-7007, Office of Nuclear Regulatory Research, Washington, DC (2010).
[28] 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).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA-TECDOC-1787, IAEA, Vienna (2016).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
[31] ELECTRIC POWER RESEARCH INSTITUTE, Hazard Analysis Methods for Digital Instrumentation and Control Systems, Rep. 3002000509, EPRI, Palo Alto, CA (2013).
[32] ELECTRIC POWER RESEARCH INSTITUTE, Operating Experience Insights on Common-cause Failures in Digital Instrumentation and Control Systems, Rep. 1016731, EPRI, Palo Alto, CA (2008).
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Managing Modernization of Nuclear Power Plant Instrumentation and Control Systems, IAEA-TECDOC-1389, IAEA, Vienna (2004).
[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-1.4, IAEA, Vienna (2009).

ABBREVIATIONS

CCF	common cause failure
HSI	human–system interface
HVAC	heating, ventilation and air-conditioning
I&C	instrumentation and control
PIE	postulated initiating event
SFC	single failure criterion

CONTRIBUTORS TO DRAFTING AND REVIEW

Burzynski, M.	NewClear Day, Inc., United States of America
Chernyaev, A.	Rusatom Automated Control Systems, Russian Federation
Dittman, B.	Nuclear Regulatory Commission, United States of America
Eiler, J.	International Atomic Energy Agency
Frost, S.	Office for Nuclear Regulation, United Kingdom
Glockler, O.	SunPort SA, Switzerland
Golub, P.	EXCEL Services Corporation, United States of America
Herb, R.	Southern Nuclear Company, United States of America
Johnson, G.	Computer Dependability Associates, LLC, United States of America
Kawanago, S.	Mitsubishi Heavy Industries, Japan
Lamb, C.	Sandia National Laboratories, United States of America
Mouly, P.	Rolls-Royce Civil Nuclear, France
Nguyen, T.	Électricité de France, France
Pickelmann, J.	AREVA NP GmbH, Germany
Rounding, A.	Amec Foster Wheeler, United Kingdom
Sivokon, V.	Rusatom Automated Control Systems, Russian Federation
Tikku, S.	SNC Lavalin, Canada
Turi, T.	MVM Paks II, Hungary
Wood, R.	University of Tennessee, United States of America

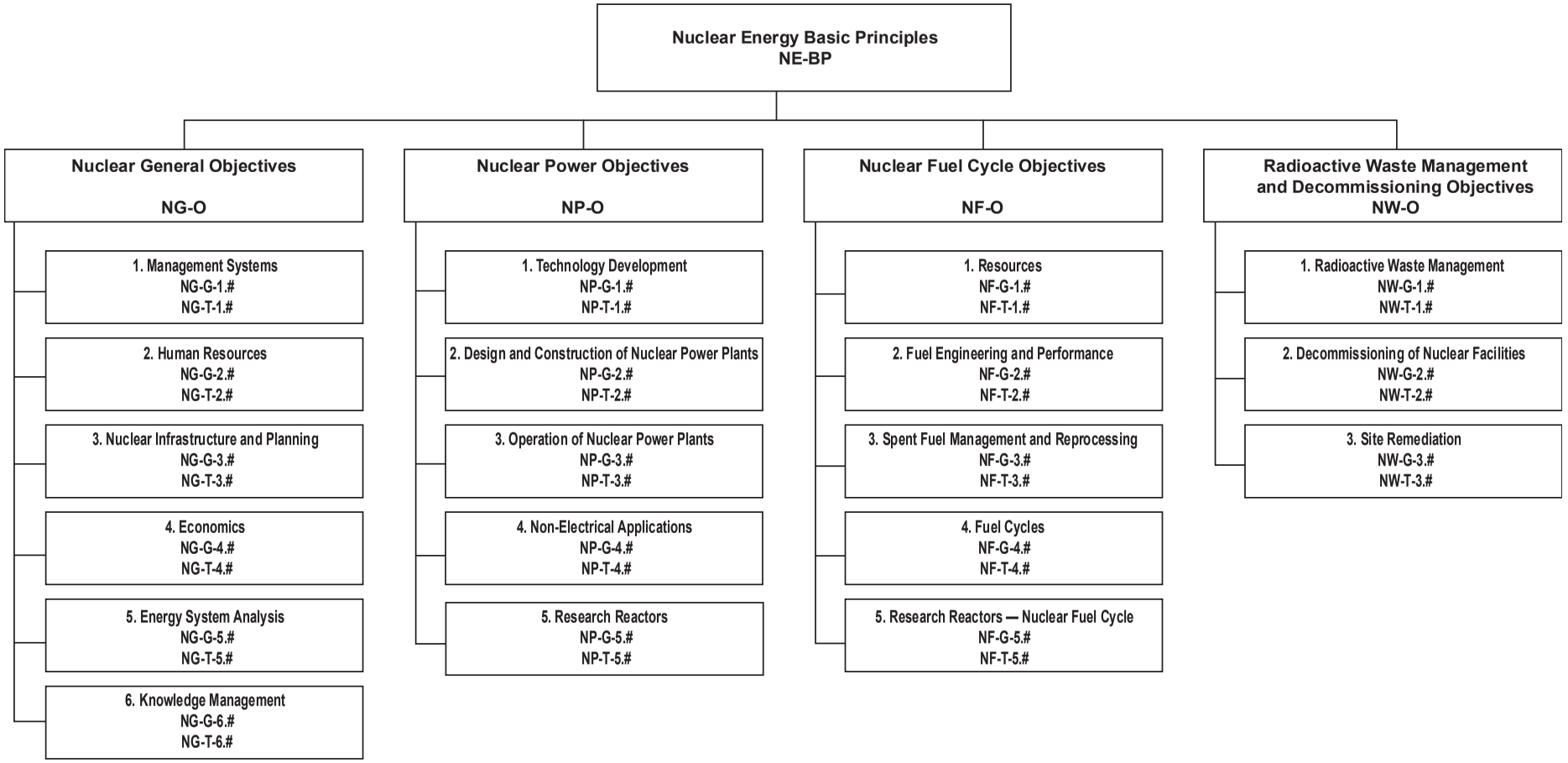
Technical Meeting

Grenoble, France: 27–30 September 2016

Consultants Meetings

Vienna, Austria: 7–11 December 2015, 30 May – 3 June 2016, 13–17 March 2017

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. 25

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.

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: www.renoufbooks.com

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

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: 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: formedit@formedit.fr • Web site: www.form-edit.com

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: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

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: www.alliedpublishers.com

Bookwell

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

JAPAN

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.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: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

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: www.renoufbooks.com

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

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 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–102718–4
ISSN 1995–7807