WORLD NUCLEAR ASSOCIATION

I&C Modernization: Current Status and Difficulties

Cooperation in Reactor Design Evaluation and Licensing – Digital Instrumentation and Control Task Force

Title: I&C Modernization:
Current Status and Difficulties
Produced by: World Nuclear Association
Published: September 2020
Report No. 2020/009

Cover Photo: ©Framatome

Foreword

The Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group was created in 2007 to promote the development of a worldwide regulatory environment where standardized reactor designs can be widely deployed without major design changes at a national level.

The Digital Instrumentation and Control Task Force (DICTF) of CORDEL was set up in 2013 to investigate key issues in digital I&C related to the licensing of new or operating nuclear power plants, and to collaborate with the International Electrotechnical Commission (IEC) and the Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC)[1].

The need for I&C modernization in nuclear power plants, part of the worldwide changeover from analogue to digital automation technology, stems from the progressively longer lifetime of the plants and the increasingly restricted life span and faster obsolescence of I&C components. As most of the main I&C related codes and standards (C&S) are focused on new nuclear power plants, their adaptation to the modernization of I&C systems of operating plants presents a challenge. Utilities have many things to consider when undertaking modernization including:

- the scope of events to be managed by the design, such as complex failure scenario, I&C Common Cause Failure (CCF), cybersecurity threats;
- implementation of new I&C functions in existing I&C systems;
- increasing complexity of digital systems and, as a consequence, a significantly more difficult licensing process;
- lessons learned from previous modernization projects.

This paper builds upon the ideas and experiences shared at an I&C modernization workshop in Erlangen, Germany in October 2019 organized by CORDEL and the International Atomic Energy Agency (IAEA). It provides an overview of the current status regarding I&C modernization and identifies the main difficulties the nuclear industry is facing. CORDEL DICTF intends to continue its work on I&C modernization through, for example, the development of checklists and more in-depth papers on selected topics.

Acknowledgement

The CORDEL Secretariat of the World Nuclear Association expresses its gratitude to Johannes Pickelmann (Framatome), Mauri Viitasalo (TVO), Mark Burzynski (SunPort) and Warren Odess-Gillett (Westinghouse) for drafting this report, and to colleague Richard Petrie for his diligent work in its design.

[1] As the successor to the Multinational Design Evaluation Programme Digital Instrumentation and Control Working Group

Contents

Annexes

List of acronyms

BOP	Balance of Plant
CM	Configuration Management
CNRA	Committee on Nuclear Regulatory Activities (of the OECD/ Nuclear Energy Agency)
CORDEL	Cooperation in Reactor Design Evaluation and Licensing
DICTF	Digital Instrumentation and Control Task Force
DICWG	Digital Instrumentation and Control Working Group
DiD	Defence-in-Depth
DiD&D	Defence-in-Depth and Diversity
EPRI	Electric Power Research Institute
FFF	Form, Fit and Functions
FPGA	Field Programmable Gate Array
HVAC	Heating, Ventilation and Air Conditioning
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IT	Information technology
MDEP	Multinational Design Evaluation Programme (NEA)
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OEM	Original Equipment Manufacturer (includes suppliers for NSSS and BOP)
PIE	Postulated Initiating Event
REM	Requirements Engineering and Management
RIL	Research Information Letter
SC	Safety Class
SDO	Standards Development Organization
SE	System Engineering
SSCs	Structures, Systems and Components
V&V	Verification and Validation
WNA	World Nuclear Association

Definitions

Unless otherwise stated, terminology used is defined according to the IAEA Safety Glossary, Revision 2018 [1].

Key words

Instrumentation and Control, Modernization, Replacement, Upgrade, Re-engineering, I&C Equilibrium

Executive Summary

I&C modernization in nuclear power plants, part of the worldwide changeover from analogue to digital automation technology, is driven by the progressively longer lifetime of the plants and the increasingly restricted life span and faster obsolescence of I&C components. Challenges faced by operators, suppliers and regulatory authorities are quite similar worldwide. Various papers have been issued on the lessons learned from I&C modernization by organizations, such as the International Atomic Energy Agency (IAEA), International Electrotechnical Commission (IEC), and Electric Power Research Institute (EPRI). This paper, prepared by the World Nuclear Association, does not aim to replace their findings but rather focuses on recent experiences of the industry, and aims to raise awareness of the challenges a project might face. In the future, the CORDEL Digital I&C Task Force (DICTF) will continue working on the I&C modernization subject and intends to provide specific guidelines on selected items through checklists and in-depth papers on selected topics.

Presently, more than 50% of nuclear power plants (NPPs) are more than 30 years old (Chapter 1). For many of these, the operator plans to extend the life of the plant. Several previous I&C modernization projects resulted in major challenges for everyone involved. In some cases this led to considerable time delays, cost increases and most importantly, to a loss of confidence in the industry. The CORDEL DICTF is convinced that early consideration of the main challenges during initial studies or planning phases provides benefits for all stakeholders and leads to increased confidence in the industry.

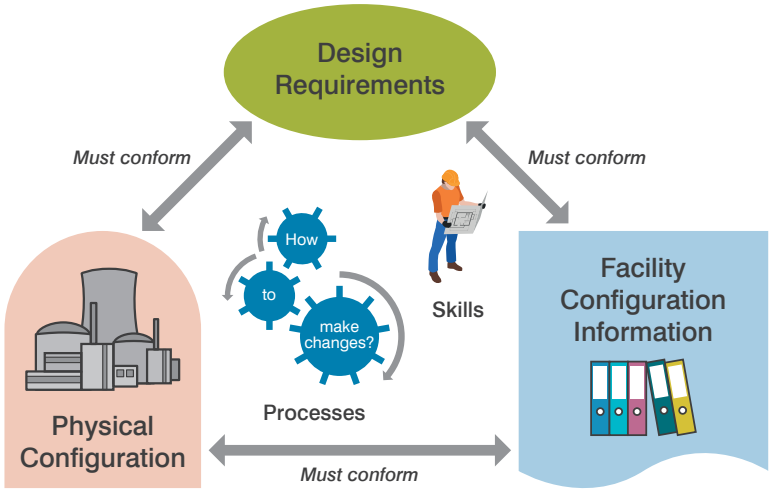
As with other areas of the nuclear field, it is valuable to create an internationally uniform basis for the approach to I&C modernization. Chapter 2 clarifies the wording related to different types of I&C modernization, from replacement to upgrades and implementation of new components and systems. Depending on the type of modernization, operators in particular should weigh up the advantages and disadvantages in connection with their particular situation and establish clearly the reasons to modernize I&C at their plants.

The scope of modernization is directly deduced from the plant needs and the requests of the national regulator. Annex A provides a brief overview of the general factors concerning the drivers and a discussion of the lifetime management of an NPP. To define the essential elements of the supply scope, CORDEL DICTF proposes to use the I&C equilibrium as introduced by IAEA on configuration management (Figure overleaf).

Codes and standards, as well as guidelines, set the framework for NPP engineering. Chapter 3 provides an overview of the documents published in the past decade relevant to I&C modernization. Annex B provides more detailed information on the normative references to be taken into account and gives a short overview of the available documents, their intent and quotes the most important content.

The I&C equilibrium concept as shown in the Figure below considers the three elements of design requirements, facility configuration information and physical configuration supplemented by processes on “how to make changes” and the required skills. A balance of the configurations represents an ideal state during the plant lifetime. In general, modernization can be interpreted as a transition from one steady state of the equil ibrium to a new steady state[2]. Chapter 4 provides explanations of the five elements and corresponding examples.

[2] The Equilibrium Concept considers that there are three elements that need to be in equilibrium: design requirements, facility configuration information and physical configuration. A balance of the three configurations represents an ideal state during the plant lifetime. Chapter 4 explains these states in more detail.



A simplified diagram of I&C Equilibrium

Building on the I&C equilibrium, Chapter 5 gives examples of typical causes of difficulties based on the experience of CORDEL DICTF members. This chapter represents the core of the paper. Even though stakeholders might face the mentioned topics to different degrees, World Nuclear Association recommends they are examined and assessed for the plant-specific case. The intention of this chapter is to highlight typical challenges and to provide recommendations to ensure these issues are being taken into account when planning the intended modernization.

1 Introduction

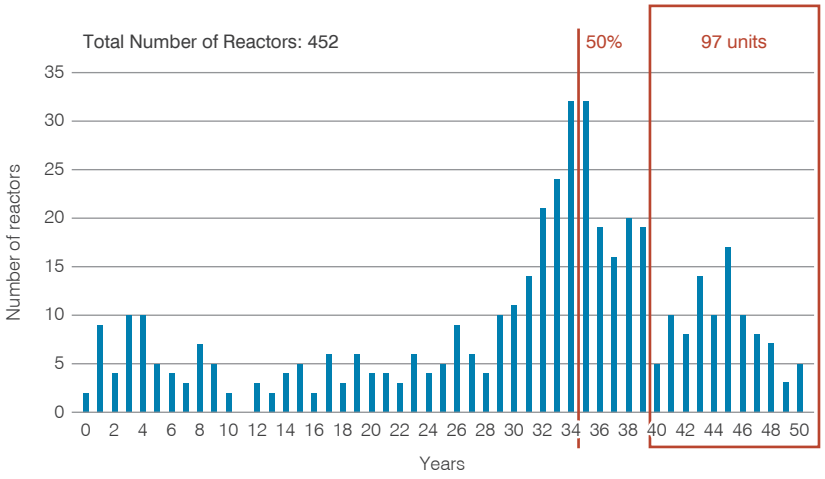


Figure 1. Age of operating reactors (IAEA, May 2019)[3]

1.1 Background

As of May 2019, more than 50% of the 452 worldwide operational nuclear power plants (NPPs) are more than 30 years old (97 units have been in operation for between 40 and 50 years) – see Figure 1. The age of the plants, the envisaged lifetime extension, component obsolescence, advantages of new technological achievement, *etc.* lead to the need for NPP I&C modernization.

Besides the opportunities associated with plant improvement and upgrading, the execution of I&C modernization projects[4] encounters many challenges that need to be addressed. The most challenging aspect for the nuclear industry is the licensability of the systems, structures and components (SSCs) to be used for modernization. Lessons learned from previous projects have shown that the use of new or unknown equipment/technology has led to unexpected pitfalls, which should be addressed to ensure the smooth and timely completion of a modernization project. In spite of many modernization projects that have been completed in a timely manner and successfully, the nuclear industry has experienced various difficulties. Many plant operators have today strong concerns regarding I&C modernizations. The WNA CORDEL Digital I&C Task Force (DICTF) is convinced that early consideration of the main challenges during studies or planning phases provides benefits for all stakeholders. Sharing our experiences and lessons learned with the nuclear industry, we are convinced that future modernization projects can be carried out successfully. This experience has led to the DICTF decision to work on the subject.

1.2 Objective

Several publications in the nuclear industry have already identified the risks and opportunities for I&C modernization. This report on I&C modernization by WNA CORDEL DICTF intends to provide an overview of the technical and organizational needs and requirements given by standards development organizations (SDOs) specific for I&C modernization (see Annex A) and to identify the main difficulties the nuclear industry faces. The report will be used to support future discussions with key stakeholders in the nuclear industry including regulators, operators and vendors of safety and operational I&C.

[3] http://www.iaea.org/pris/

[4] Types of I&C modernization projects are described in Section 2.

Although every NPP I&C modernization project is unique and has to be managed individually, this report provides an overall discussion on the topic. The given structure of topics could be used for harmonization in order to provide a basis for international exchanges of lessons learned. To promote the highest level of safety and to improve public perception and trust for nuclear power, in combination with the right balance between quality, schedule and costs, it is essential for the nuclear industry (utilities and suppliers) to work together. This report is addressed to all stakeholders of the I&C engineering life cycle (including maintenance and operation) and the disciplines interfacing with I&C design. To strengthen the cooperation of the various disciplines involved in I&C modernization, the main challenges have to be properly acknowledged. DICTF is looking forward to refining the joint work and welcomes future exchanges on this topic.

2 Types of I&C Modernization

New nuclear power plants are built based on a generic design of the original equipment manufacturer (OEM)[5] - typically reflecting state-of-the-art technology and safety requirements. Yet for modernizations in existing operating plants there is a need to deal with the transition from the original overall plant design (reflecting state-of-the-art technology and safety requirements of decades ago) to a "digital" state fulfilling current (safety) requirements.

Planning and implementing an I&C modernization project requires a plant-wide concept for lifetime management, as described in Annex A: Generic Approaches for I&C Modernization. The plan for the I&C Lifetime Management identifies the priorities of the I&C SSCs to be modernized within a certain time frame. I&C modernization could be executed in different ways. The decision for the type of I&C modification (modernization) results mainly from the scope of changes.

IAEA TECDOC-1016 [2] introduces the term "modernization" and organizes it into three types of change regarding I&C systems:

- the ***replacement*** of ***old*** systems and components,
- the ***upgrading*** of ***old*** systems and components, and
- the ***implementation*** of ***new*** systems and components.

The term "replacement" is used when an existing component or system is replaced with a new or improved technology but there is no change in its capabilities.

The term "upgrading" is used when an existing component or system is replaced with a new or improved technology version and this leads to increased capabilities.

The term "new implementation" is used when a system with new functionalities is implemented in the plant.

The scope of these modernizations covers a wide range of activities. It includes the modernization of equipment in operating plants and the modernization of equipment and designs in delayed constructions. It covers large and complex systems, small systems, and individual components in systems. It also covers the complete replacement of all the I&C equipment in a plant. It applies to the full range of I&C systems including protection, control and information systems that a plant needs throughout its lifetime.

Note: An "I&C modernization project" is not limited to one type of the changes described above. Depending on the scope of modernization, different approaches can be applied for selected SSCs.

2.1 Replacement vs New Implementation

The scope of I&C modernization can range from a single module replacement to modification of the overall plant design concept (*e.g.* installation of additional safety trains).

I&C modernization (replacement/ new implementation) can be realized using one or more of the following strategies (referred to also as I&C modernization types):

1. Continued spare parts replacement;
2. Form, fit and function (FFF) module replacement (retrofit);
3. I&C rack replacement;
4. New I&C cabinet implementation;
5. New I&C systems implementation.

[5] OEM includes suppliers for nuclear steam supply systems (NSSS) and balance of plant (BOP).

Figure 2 provides an overview of the different types of I&C modernization (replacement/new implementation) and subjective analysis of the pros and cons and the opportunity costs[6] (OP) of each type. The figure deals exclusively with the replacement/modernization of the process control systems (I&C layer 2). Depending on the scope of the project, this may also involve changes at the level of sensors (I&C layer 0), field control devices (I&C layer 1) and the supervisory control and information systems (I&C layer 3)[7].

Types 1 and 2 require no work on overall I&C architecture, as the existing function allocation and I&C design basis concept (including defence-in-depth, DiD) will remain valid.

The other types could require an update of the reliability, failure and hazards analyses of the overall I&C architecture. This is for example the case 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 types 3, 4 and 5, one needs to distinguish between:

- One-to-one implementation of a new single I&C system; and
- Integration of several discrete "process I&C systems[8] " to a new single I&C system(s).

The integration 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, but even a one-to-one replacement could be a concern. This might require splitting one single system into several discrete systems. In the case of replacement of a protection system, a diversity strategy (not considered in the original plant design), internal or external to the system, might be considered.

The scope for an I&C upgrade project can range from single components to an entire I&C system. The different options of modernization strategies discussed previously can therefore be extended to include component upgrade and digital I&C system(s) upgrade.

Component upgrade focuses on the upgrade of single modules for which an OEM supplier offers a follow-up component[9] as replacement for obsolete equipment. These components typically do not fulfil the FFF criteria as they might include additional or slightly modified functionalities or rely, for example, on different interface technology. Compared with options 1 and 2, additional analysis or tests might be required to demonstrate compatibility.

As more and more digital I&C systems come into operation in NPPs worldwide, it is necessary to discuss digital I&C system upgrades. The aim is to provide the operator with an upgrade of existing but outdated digital components/platform to an up-to-date configuration (hardware in combination with software), without replacement of the whole system (see Section 5.3.7 for more details).

[6] Regarding: *What does it imply to choose one option over the other?*

[7] Following the I&C Layer model as described in Section 4.3

[8] In this context, the composition of a "process I&C system" relates to (a) functional task(s), not on the basis of the defence-in-depth concept of the plant/I&C architecture.

[9] A follow-up component can be a later or subsequent version of the module.

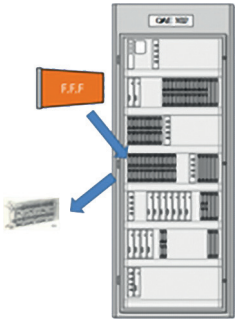
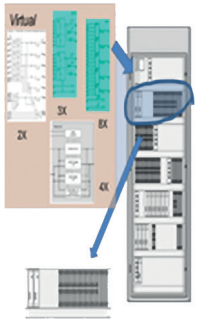
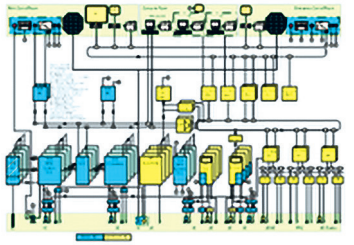
	(1) Spare parts replacement	(2) FFF module replacement (retrofit)	(3) I&C rack replacement	(4) New I&C cabinet implementation	(5) New I&C systems implementation
					
PROS	• Cost effective in short time • Fast replacement during outage • No effect on documentation • Increased lifetime of existing system	• Reverse engineering limited on module level • Fast replacement • Small effect on documentation	• Equipment frame treated as black-box • Similar interface within cabinet • Use of existing I&C products/ platform	• Same footprint • Replacement during a single outage • Revolve safety deficiencies • Improve operation	• Cost effective in the long term (lifetime extension program) • Stringent DiD concept implementation • Interface optimization
CONS	• Spare parts costs growing • Dependability of few skilled people • Limited availability of components • Limited improvements in failure rate of existing system	• New product development + qualification • Lack of knowledge on installed products • High investment on clone product • OEM intellectual properties • No adverse impact to original system	• Reverse engineering full equipment frame • Less improvement on optimization • Medium effect on documentation • Management of interfaces • Cybersecurity (partial)	• More complex redesign/ interfaces • Reverse engineering for new I&C system • New documenation • New licensing • Cybersecurity • Shortened product life cycle of digital components	• Complex replacement + reverse engineering for whole plant • Challenge on regulatory approval • Extensive quantity of stakeholders with necessity of comprehensive knowledge
OP	• No maintenance improvement • Minor integration of the younger engineer generation • No improvement of the existing documentation • Increased lifetime of new modules	• No improvement on internal wiring, power supply, monitoring • Low use by other operators	• No alternative of the system architecture/mapping of functions to I&C cabinets • No consideration of additional independence requirements	• Expiry of the existing licence • Extensive regulatory requirements • New technology – need for training/loss of older engineer generation	• Impact on overall plant principles incl. DiD, Human-Machine-Interface, Overall Architecture, etc. • “Heart surgery on the living body”

Figure 2. Comparison of I&C modernization types for replacement/new implementation (Pros/Cons/Opportunity costs (OP))

2.2 Reasons to Modernize

The aim of the plant lifetime management plan[10] is to monitor the plant condition during the entire operating phase in order to ensure the required overall plant effectiveness, which is defined as the product of the factors: availability, reliability and quality. The availability factor[11] is reduced by the recovery time such as: non-availability of spare parts/errors in the system/discontinued support.

In addition, there may be other reasons for which I&C modernization is required. The reasons for modernizing I&C equipment have to be identified clearly in order to select the right modernization type. Typical reasons include one or more of the following objectives:

- Address obsolescence;
- Ensure and improve reliability;
- Fix existing maintenance problems;
- Improve maintainability;
- Reduce workload;
- Shorten outage time or simplify plant start-ups;
- Provide better control leading to fewer plant upsets;
- Use common digital platforms;
- Support workforce plans.

It is also important to consider enhancements that may be incorporated into I&C modernization projects. Some typical enhancements that should be considered include one or more of the following changes:

- Elimination of single point failures;
- Ease of maintenance;
- Reduction or elimination of testing;
- Automation of testing;
- Upgrade of instrumentation;
- Redundant critical measurements;
- Smart transmitters for ease of calibration;
- Switches to transmitters (*e.g.* pressure, flow, *etc.*);
- Additional information available to operations and maintenance through the human-machine interface;
- Improved manual or automatic diagnostics of the control system as well as process for ease of troubleshooting.

It is important to consider these factors at the start of the project (concept stage) to avoid the problems that come with scope changes during project implementation.

[10] See Annex A – Section A-2. Lifetime Management

[11] Availability = MTBF (mean time between failures) / (MTBF (mean time between failures) + MTTR (mean time to restoration)

3 Guidelines, Codes and Standards for I&C Modernization

International SDOs and various institutes have published several reports about I&C modernization in the past 20 years. To provide a rough overview, the most relevant are listed in this chapter. The following list does not include all the documents published in this area.

Annex B provides more detailed information on the normative references to be taken into account, along with a short overview of the available documents, emphasizing their intention and quoting the most important content.

3.1 IAEA - International Atomic Energy Agency

The IAEA Specific Safety Requirements SSR-2/1 [3] document represents the top level of the international normative references for I&C, with the focus on safety design of existing and new NPPs. It identifies requirements to be considered for new plant design and modernization projects. SSR-2/2 [4] deals with the commissioning and operation of NPPs. It specifies the need to perform lifetime management of the overall plant including its systems, structures and components. It recommends that: "Where applicable, the operating organization shall establish and implement a comprehensive programme for ensuring the long term safe operation of the plant beyond a time-frame established in the license conditions, design limits, safety standards and/or regulations."

The IAEA Specific Safety Guide SSG-39 [5] could be seen as the top-level document for engineering of I&C for NPPs. Section 1.14 says: "The guidance applies to the design of I&C systems for new plants, to modifications of existing plants and to the modernization of the I&C of existing plants." The "Modification" chapter provides more detailed information on the specific subject. SSG-30 [6] deals with the "Safety Classification of SSCs in NPPs". It points out that this "may not be applicable to existing plants built with earlier classification principles" and that individual states must decide on the methodology applied to such plants.

The IAEA Safety Series reports (*e.g.* Nuclear Safety Guides, Nuclear Power Objectives) and related TECDOCs have the objective to provide guidance and recommendations on controlling activities. A broad set of documents have been published in the past decades. The most relevant ones for DICTF are:

- IAEA NS-G-2.3 "Modification to Nuclear Power Plants" [7], published in 2001, which provides guidance and recommendations on controlling activities related to modifications at NPPs. It is not an I&C-specific guide but it deals with the modification of structures, systems and components such as I&C.
- IAEA NP-T-1.13 "Technical Challenges in the Application and Licensing of Digital I&C in NPPs" [8], published in 2015, which has the goal to present the technical challenges regarding the transition from analogue to digital I&C from the perspective of licensing digital I&C systems in NPPs. Its final objective is to help industry stakeholders move towards effective resolution and a more common position on these technical issues.

- IAEA TECDOC-1016 "Modernization of instrumentation and control in nuclear power plants" [2], published in 1998, is still relevant and covers a huge set of those topics which are of main interest for DICTF such as strategy, managerial aspects, design criteria, engineering requirements and constraints, and licensing aspects.

3.2 IEC - International Electrotechnical Commission

Below the IAEA in the hierarchy of international normative references for nuclear I&C, IEC SC45A represents the main international SDO providing requirements for the engineering of I&C systems (including I&C modernization). IEC is organized by levels (level 1 to 4).

IEC 61513 [9] is the first-level IEC SC45A document, tackling the issue of general requirements for systems. It is the entry point of the IEC SC45A standard series regarding nuclear I&C safety systems. According to its Section 1.2, the standard "applies to the I&C of new nuclear power plants as well as to I&C upgrading or back-fitting of existing plants. For existing plants, only a subset of requirements is applicable and this subset should be identified at the beginning of any project". The application of the IEC SC45A standards of the subsequent levels (*e.g.* IEC 61226, IEC 60880, IEC 60709, *etc.*) should be defined during the project planning phase.

The technical report IEC TR 62096 "Guidance for the decision on modernization" [10] belongs to the fourth level of SC45A documents. It is intended to support owners of an NPP in the decision-making process and in the preparation for partial or complete modernization of the I&C systems. It provides a summary of the motivating factors for I&C modernization, the principal options for the elaboration of different scenarios for I&C modernization, the technical and economic criteria for the selection of a long-term I&C strategy and the principal aspects to be taken into account for a detailed technical feasibility study.

3.3 EPRI - Electrical Power Research Institute

In recent years EPRI has published several guidelines such as "Digital Instrumentation and Control Design Guide" (2014), "Instrumentation and Control Strategies for Plant-Wide and Fleet-Wide Cost Reduction" (2007), "Guideline for Performing Defence-in-Depth and Diversity Assessments for Digital Upgrades" (2004), "Advanced Nuclear Technology: Guidance and Methodologies for Managing Digital Instrumentation and Control Obsolescence" (2015) and "Instrumentation and Control, Human System Interface, and Information Technology Requirements Project Plan for Nuclear Power Plant Long-Term Operation" (2010). The more detailed information of EPRI documents mentioned here can be found in Annex B with proper referencing.

3.4 Others

Other regulators, organizations and institutes such as the US Nuclear Regulatory Commission (NRC), the Committee on Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency, the Institute of Electrical and Electronics Engineers (IEEE) and Energiforsk have published reports related to I&C modernization:

- IEEE in 2014 published a guide for assessing, monitoring, and mitigating ageing effects on class 1E equipment used in NPPs (IEEE Std 1205).
- In 2014 the Idaho National Laboratory also published a report on "Advanced Instrumentation, Information, and Control Systems Technologies: Digital Technology Business Case Methodology Guide" (INL/EXT-14-33129).
- Energiforsk in 2015 issued its Nuclear Safety Related Instrumentation and Control (ENSRIC) strategy plan in order to find cost- and time-effective methods to extend the lifetime of the present analogue systems and the asset management of already installed digital platforms. In 2016 it published reports on "Replacing Obsolete Nuclear Instrumentation and Control Equipment" and "Upgrading to Modern Computerized I&C Systems". In 2018, a new report, "Safety Demonstration Plan Guide", was published. This report suggests a structured approach to carry out planning and execution of safety demonstration/licensing for modernization and new build projects (including digital I&C systems).

4 I&C Modernization - Scope of Modernization (I&C Equilibrium)

The scope of modernization is directly deduced from the plant needs (identified by the plant/I&C lifetime management plan) and the requests of the national regulator (Annex A).

To define the essential elements of the supply scope, WNA proposes the use of the I&C Equilibrium Model. This model is derived from the Configuration Management Equilibrium Model, for example as described in IAEA Safety Report Series No. 65 "Application of Configuration Management in Nuclear Power Plants" [11] and IAEA TECDOC-1335 "Configuration Management in Nuclear Power Plants" [12]. The concept considers that three elements need to be in equilibrium: design requirements, facility configuration information and physical configuration. A balance of the three configurations represents an ideal state during the plant lifetime. Modernization could be seen as a transfer from one configuration version (state) to the next. To cover this transfer the concept is extended to the following elements: work processes (how to make changes) and staff skills – see Figure 3.

4.1 Design Requirements

The "Design Requirements" element specifies "what is required to be there".

According to ISO/IEC Directives part 2, 2004, 3.12.1 (see IEC TR 62096 [10]), requirements are "expression in the content of a document conveying criteria to be fulfilled if compliance with the document is to be claimed and from which no deviation is permitted."

The design of safety I&C systems is based on an extensive set of design requirements specified by the regulators, the utility and the involved disciplines such as process and safety, I&C architecture/system, supply systems (including electrical power supply, HVAC, plant security, *etc.*), mechanical design, plant operator and maintenance team.

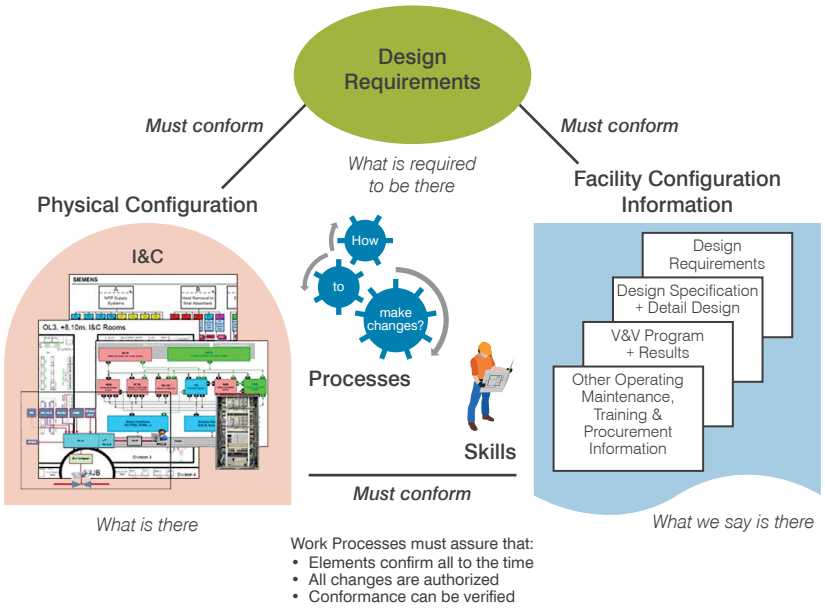


Figure 3. I&C Equilibrium Model

According to IEC TR 62096 [10], IEC SC45A documents distinguish between the following types of requirements:

(1) **Safety requirements** – Requirements imposed by authorities on the safety of the NPP in terms of impact on individuals, society and environment during the NPP life cycle.

(2) **Functional and performance requirements** – Functional requirements state what actions the system must take in response to specific signals or conditions. Performance requirements define features such as response times and accuracy.

(3) **Operational requirements** – Requirements on the operational capacity and ability of the plant imposed by the owner.

(4) **Plant design requirements (plant constraints)** – Technical requirements on plant general design for the fulfilment of the safety requirements and operational requirements of the plant.

(5) **I&C system design requirements** – Requirements on individual systems to give a design of the complete plant fulfilling the overall plant design requirements.

(6) **Equipment requirements** – Requirements on individual items of equipment to fulfil the demands of the system design.

(7) **IT security requirements** – Requirements on activities and measures for the prevention of, detection of and reaction to malicious acts by digital means (cyberattacks).

The identification of the design requirements shall be based on a systematic approach with the aim that all relevant requirements are known and understood in a necessary degree of detail and all involved stakeholders have a sufficient common understanding of the requirements.

Each requirement shall fulfil at least the following (requirement) quality criteria, such as:

- Identifiable: each requirement has a unique identifier;
- Singular: each requirement statement includes only one requirement;
- Necessary: each requirement is necessary to fulfil the function of the system;
- Understandable: the intended reader (*e.g.* design team, verification and validation (V&V) team) can understand the requirement;
- Implementation free: each requirement shall be stated in a manner that is solution independent – this will permit consideration of different design implementations;
- Validation: each requirement can be demonstrated by testing and/or analyses and/or inspection;
- Unambiguous: each requirement can be interpreted in only one way;
- Feasible: each requirement is technically achievable, does not require major technology advances, and fits within system constraints with acceptable risk;
- Consistent: each requirement is free of conflicts with itself and with other requirements;
- Complete: each requirement contains all necessary information;
- Traceable: each requirement can be traced to its stakeholder requirement.

Requirements are documented in natural language. Therefore it is important to use a common, aligned terminology when setting requirements.

It is beneficial to understand from the beginning what is possible for the modernization project. Modern digital I&C technology can provide many beneficial features that are not available or possible in analogue technology. It can be beneficial to go outside the nuclear industry to evaluate feasible options, since other industries have performed digital modifications for years. It is important to define the functionality required in the system, decide upfront on necessary supplier documentation, and clearly identify this in the specification.

It is often helpful to create an onsite digital modification team to provide focus and be educated on digital issues and products.

Clear and accurate specifications are critical to project success. It is therefore essential to provide enough time to write a good specification, review it, and ensure the project schedule is realistic in order to avoid a common scenario that might lead to project failure. Even if the specification is issued late, the project is always expected to meet the original completion schedule. Above all, the associated simulator upgrades need to be done, since this is the first stage of the project to be implemented.

The changes required for the plant probabilistic risk assessment (PRA) will need to be considered for those plants that use the PRA to support regulatory decisions or online maintenance scheduling. The project scope will need to include the required reliability or fault tree analyses at the necessary level of detail to be integrated into the existing PRA models.

4.2 Facility Configuration Identification

The element “Facility Configuration Identification” specifies “what we say is there”.

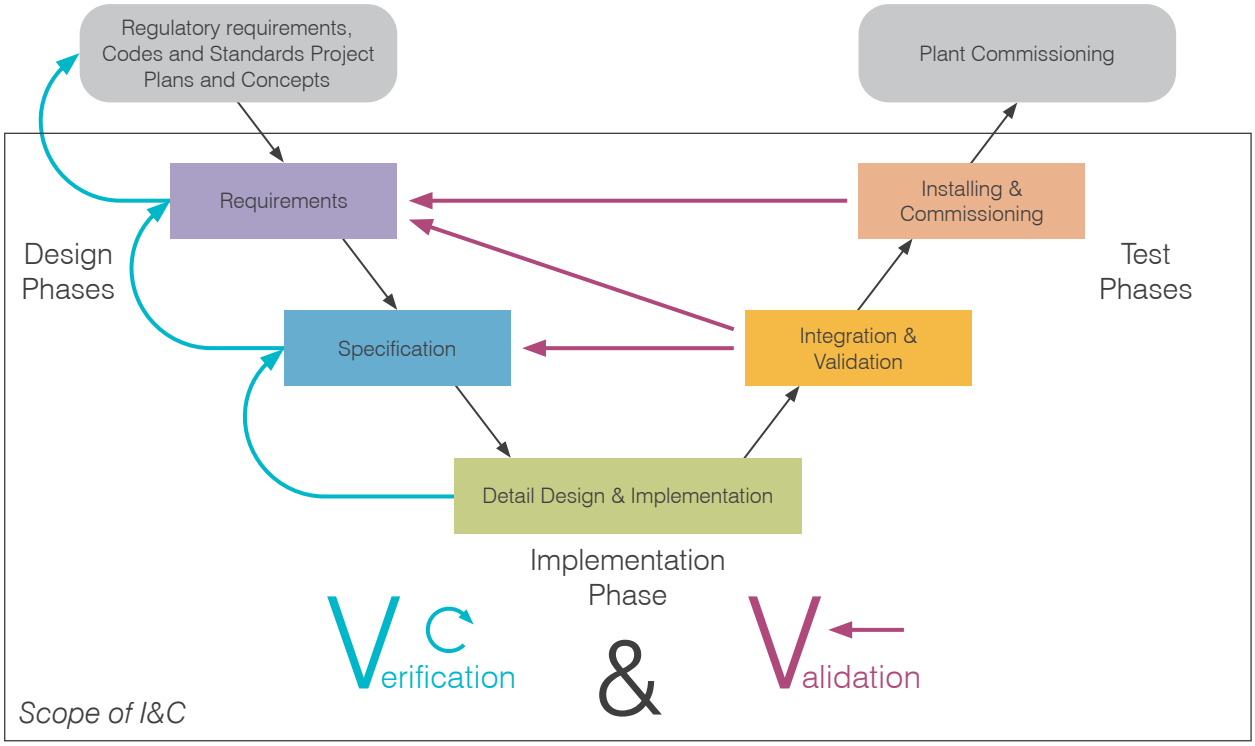


Figure 4. V-model (example)

Codes and standards such as IAEA SSG-39 [5] or the IEC SC45A level 1 standard IEC 61513 [9] introduce the concept of a safety life cycle for the overall I&C architecture, and a safety life cycle for the individual systems. They identify a systematic approach for a typical I&C engineering life cycle covering the requested design activities resulting in documentation/data[12].

The design process is defined as a sequence of phases. Each phase consists of a set of inputs and outputs (by means of documents or data). An effective development process should define a specific set of documents to be provided at each phase covering the documents expected by the regulator for licensing. Safety I&C SSCs designed and installed in NPPs must be fully reproducible. This implies, for operating plants, that the running component design is thoroughly backwards traceable through the original engineering life cycle of the OEM and the documentation of all modifications carried out previously. This includes the documentation of the primary requirements - the "know why", the established basic and detailed design (including the functional specification and regulatory basis for the design) and the demonstration of the integration and installation. The "V-model" example shown in Figure 4 is a useful alternative view of a sample engineering life cycle. This model illustrates the relationship between phases of the systems engineering life cycle starting with the design phases through the implementation phase up to the test/ commissioning phases.

To secure the balance of the I&C equilibrium the released I&C documentation, including incorporation of all modifications so far installed in the SSCs, should be available in a legible manner.

[12] The illustrated life cycles are not the only ones possible. National regulators might have their own definition of life cycles and documents.

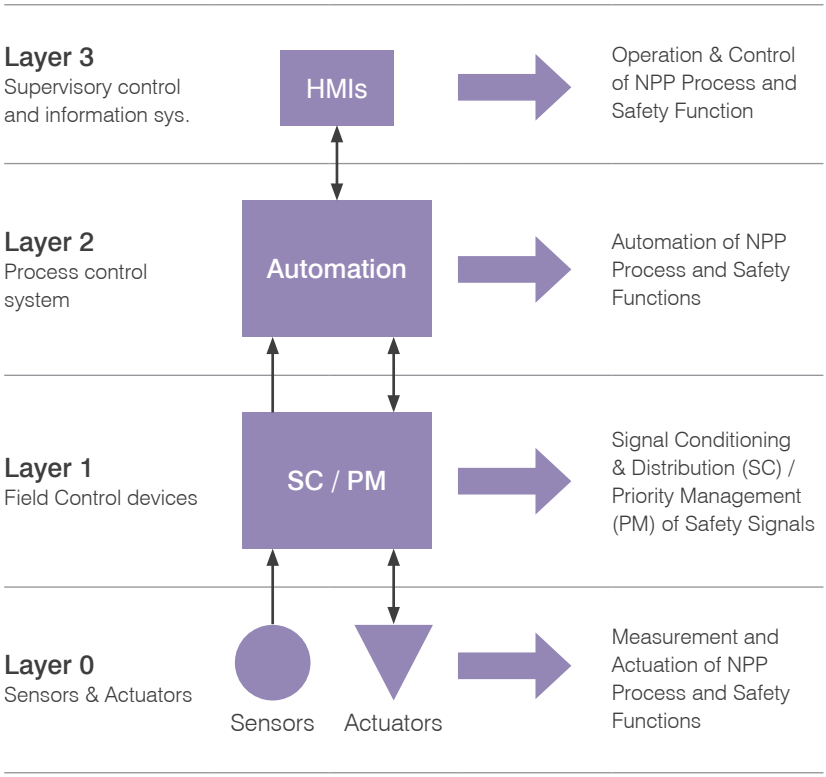


Figure 5. I&C Layer Concept (according to IAEA NP-T-2.11 [13])

4.3 Physical Configuration (of I&C SSCs)

The element "Physical Configuration" specifies "what is there".

The I&C of an NPP is organized following the overall I&C architecture, which is deduced from the OEM original plant design and its defence-in-depth concept. The I&C architecture consists of a structure of I&C systems subdivided by the importance of the SSCs to safety. IEC 61513 [9] defines the I&C system as a "system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself".

The recent IAEA publication NP-T-2.11 [13], "Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants", introduces the "I&C layer concept" as shown in Figure 5. Each layer has its own design constraints.

I&C modernization considers the impacts on the whole signal chain, starting from the sensors up to automation and back to actuators plus the interface to the operation and control of the NPP, through all layers.

Following the configuration approach, it is necessary for the utility to have detailed information on components installed in the running plant. This is normally a large amount of data and should include information on the hardware and software components of all four layers, plus the information on the interfaces (cabling). In addition, for hardware components, information on their service life should be available to support lifetime management.

4.4 Work Process (for I&C Modernization)

Work processes have to be installed to provide guidance on the design, implementation, qualification and documentation of the work. Standards such as IAEA SSG-39 [5] and IEC 61513 [9] give an overview of the required management systems for the development processes. Plant-wide organizational processes such as safety culture, quality control, licensing, *etc.*, are required in addition to I&C specific processes such as[13 14]:

- I&C systems engineering life cycle – overall development process;
- I&C system verification and validation, including system analysis[15];
- I&C system requirements management and engineering;
- I&C system components qualification;
- I&C system configuration management, including change management/change control;
- I&C system installation and commissioning;
- I&C system operation and maintenance;
- I&C system cybersecurity;
- I&C system human factors;
- I&C system operator and technician training.

The complexity of the work process needs the support of management tools especially in the field of requirements engineering and configuration management. Additional tools to support the engineering life cycle are therefore recommended. The theory of "single source of truth"[16] supports the configuration control needs.

IAEA SSG-39 Chapter 2.5 [5] states: "In order to ensure safety, documentation on the design basis and related information or records relating to I&C systems important

to safety should be controlled by suitable processes, such that they are complete, clear, concise, correct and consistent over the entire life cycle for the I&C system. The management system should ensure that design basis documents and related or derived information or records are sufficient and adequate, and are maintained over time to reflect design changes or changing conditions at the plant. This includes documents and information that may be derived from the design basis documentation and that may have an impact on safety, such as procedures or manuals relating to operation, maintenance or modification of such systems."

The implementation and execution of the specified processes are to be periodically audited by independent organizations.

Various SDOs recommend starting modernization with feasibility studies. As an example, IEC TR 62096 Chapter 6.3 [10] distinguishes between generic feasibility studies (covering the modernization scope and the time frame – see Annex A on life-time management plan) and *subsequent* feasibility studies focusing primarily on the technical aspects of the feasibility.

A technical feasibility study should consider (at least) the evaluation of:

- As-built documentation/installation/data (review of as-built functional and physical requirements/design documentation/design data applied for the licensing basis – including check for completeness, implemented modifications and inspection of the installed SSCs and interfaces);
- Condition of installed SSCs (obsolescence/availability, ageing condition, *etc.*);
- Basic input requirements (list of Postulated Initiating Events (PIEs), operational experiences, expected benefits and features, impact on safety demonstration, outage time constraints, *etc.*);
- Plant-related preconditions and goals (drivers, goals, scope, constraints for modification);
- Functional requirements including function allocation (specification and categorization of I&C functions to be modernized, allocation of I&C functions to I&C SSCs under consideration of defence-in-depth and diversity, operating and maintenance and equipment performance constraints - accuracy, response time);
- Assessment/interpretation of latest regulatory/SDO requirements (defence-in-depth, diversity, separation, *etc.*) required for licensing;
- Implementation strategy by clustering of modernization work packages (assessment on disposition of work packages, management of temporary interfaces/supply systems, *etc.*);
- Function and task analysis for the human-machine interface (consideration of process control tasks and operator's role with respect to maintenance and operation including related analysis);
- IT security constraints (plant-specific IT security management systems/separation constraints/preliminary threat analysis);
- Preliminary scope definition (quantity of sensors, actuators);
- Assessment/impact on support systems (HVAC, power supply);
- Physical allocation (assessment of spare space, footprint, cable routing, *etc.*);
- Preliminary budget costs;
- Data management/design tools;
- Licensing requirements and safety case documentation.

The typical two-step basic process for I&C modernization is illustrated in Figure 6.

[13] Depending on the type of modernization, the I&C architecture has to be planned accordingly.

[14] The organization of topics might change, depending on stakeholders' needs.

[15] Covering: hazard analysis; probabilistic safety assessments; failure mode and effect analysis; cybersecurity vulnerability analysis; response time analysis; compliance analysis, etc.

[16] Wikipedia [WL 1]: "In information systems design and theory, single source of truth (SSOT) is the practice of structuring information models and associated data schema such that every data element is mastered (or edited) in only one place. Any possible linkages to this data element (possibly in other areas of the relational schema or even in distant federated databases) are by reference only. Because all other locations of the data just refer back to the primary 'source of truth' location, updates to the data element in the primary location propagate to the entire system without the possibility of a duplicate value somewhere being forgotten."

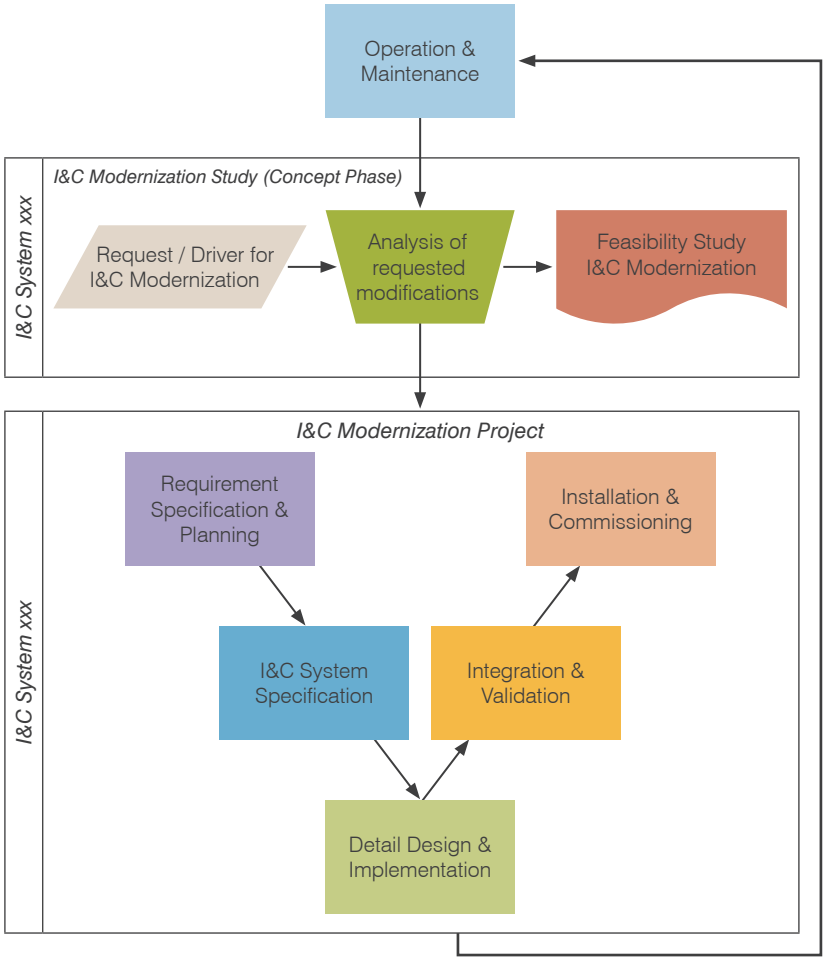


Figure 6. Basic process for I&C modernization

4.5 Staff Skills (Knowledge Management)

According to IAEA NP-T-3.12 [14]: "Knowledge Management is an integrated, systematic approach to the process of determination, collection, transformation, development, propagation, application, communication and preservation of knowledge connected with the achievement of definite purpose. … People are undoubtedly the most important component of knowledge management, since knowledge flow and transfer depends on the desire of people to share their knowledge and to use it repeatedly".

For the safe operation and modernization of an NPP, staff skills are essential. To ensure an adequate level of qualification each stakeholder should undergo training programmes to secure the knowledge of its technical and quality engineers, operators, *etc.* Through the life cycle of an NPP a plurality of technologies, changes in regulations, codes & standards, installation of new working processes *etc.* have to be managed. Keeping this knowledge base alive and ensuring the transmission to successors are essential and need to be managed by each stakeholder.

Today's main nuclear stakeholders (regulators, utilities and suppliers) are faced with the challenges of knowledge management, related to the following facts:

1. In many regions of the world the construction of new NPPs has been stopped for decades.
2. Some modernization projects have been postponed for long periods of time (mostly for economic reasons).
3. I&C equipment has a much shorter product life cycle compared to other equipment such as mechanical components.
4. New issues such as cyberthreats and other hazard scenarios arise and have to be considered in state-of-the-art I&C design.

Since the accidents at Chernobyl and Fukushima, the popularity of the nuclear industry has been noticeably impaired both in the eyes of the public and potential new young professionals[17]. Even if NPPs worldwide are starting to be valued in the climate change debate for their CO2-free generation, the potential threat for a new major event is always present. Stakeholders involved in the overall plant cycle are committed to securing the highest level of safety and quality. Consideration of new engineering methodologies (*e.g.* requirements engineering and management) and implementation of additional/advanced analysis (*e.g.* defence-in-depth and diversity analysis) considers the continuous lessons-learned process to bring NPP design to the highest level regarding safety and quality. But due to the high complexity of designs, long duration of licensing process, construction, and operation and maintenance, it is important that all involved stakeholders have the same level of requisite knowledge in order to avoid any human errors caused by a possible lack of information and knowledge transfer during the lifetime of a plant.

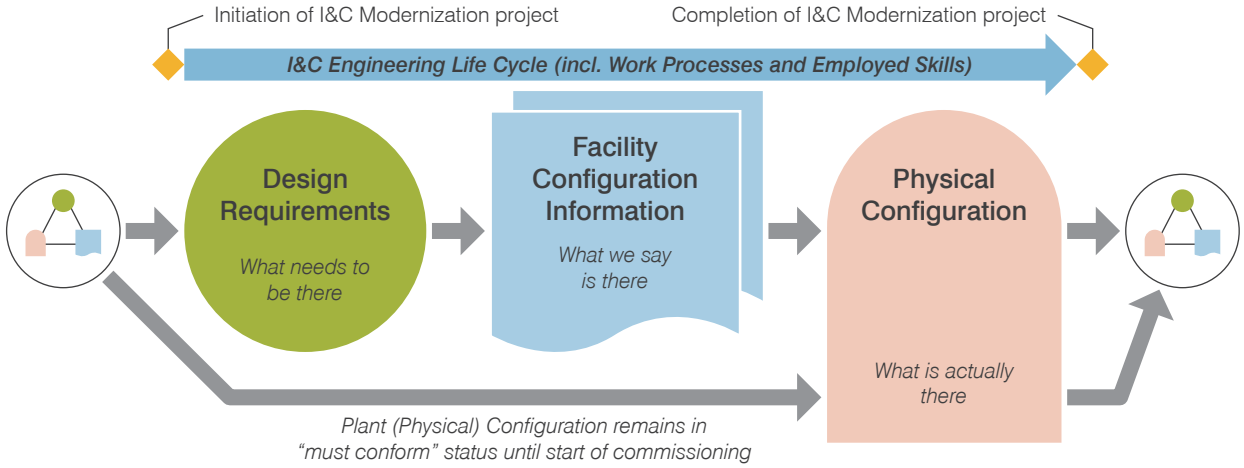


Figure 7. Maintenance of the I&C Equilibrium

4.6 Maintenance of the I&C Equilibrium

I&C modernization can be interpreted as the transition from the starting steady state of the I&C Equilibrium to the final (modernized) steady state. From the initiation of the modernization project up to its completion, the elements of the equilibrium will not conform with the others. An appropriate overall engineering process is necessary[18] to manage this transition dealing with continuous moving states (or configurations) of the plant during the stepwise implementation of the modernization, in most of the cases.

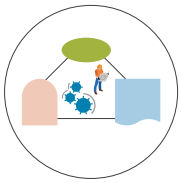
The main goal of a modernization project is to bring the plant back to the "must conform" status for all three elements. The transition is initiated by the specification (and interpretation) of the design requirements, followed by the engineering life cycle to be executed by the supplier in close cooperation with the utility to specify the facility configuration information (including the licensing of the modernization). Finally after installation and commissioning of the SSCs, the physical configuration returns to the state in which the three elements are in line with each other (Figure 7). Of course the plant (physical) configuration remains in "must confirm" status until the start of commissioning. During the I&C engineering life cycle of the modernization project, the existing design requirements and facility configuration information (documentation) remain valid until commissioning is finalized.

[17] The lack of state-of-the-art technology in an NPP is another reason young engineering professionals seem to be uninterested in making a career in commercial nuclear power.

[18] The general configuration of the plant will continue moving during the implementation of the modernization project.

5 Causes of I&C Modernization Difficulties

Presently, the DICTF has identified difficulties in modernization projects structured according to five elements (see I&C Equilibrium):



1. Design requirements;
2. Facility configuration identification;
3. Physical configuration;
4. Work process;
5. Staff skills.

Each stakeholder might face these difficulties in different degrees. This report does not intend to provide solutions or guidelines on how to deal with them. The intention is to highlight them and to provide recommendations to ensure these issues are being taken into account when planning the intended modernization.

Note: Some of the following challenges are also of relevance for new build projects.

5.1 Challenges Related to Design Requirements

This section deals with the challenges related to the changing/state-of-the-art needs of the design requirements for stakeholders.

5.1.1 Systems Engineering 1.0 (methodology applied 30 years ago)

Considering an NPP in operation for more than 30 years, it needs to be pointed out that the engineering methodologies were different at the time of construction compared to current approaches. This might be due to the fact that new information technology has been introduced over the years, but especially the industrial methods and the way of interacting between the stakeholders has changed. Regulators today require demonstration of correct and complete implementation of the design requirements. NPP operators/system integrators have been meeting this prerequisite using requirements engineering and management (REM) processes. It is necessary to document not just design solutions, but also the "know why". Plants to be modernized are challenged by the fact that very often the original design requirements of the OEM are only partly available. For the intended modernization, the original design requirements (including reverse-engineered requirements) have to be combined with the new requirements derived from the state-of-the-art design and codes and standards.

5.1.2 New/Advanced Regulatory Expectations

A further challenge related to design requirements is the new regulatory expectations based upon NPP operating experience such as near misses, investigations, lessons learned from other industries and rare NPP historical events that took place. Based on this, requirements for the design of safety I&C have been continuously reflected in the revision or creation of new codes and standards.

Design measures on separation (physical separation, electrical isolation) and diversity have been in effect for a long time, but the

requirements on the implementation level have changed. To consider these design requirements, modernization of I&C might need to introduce modifications to other disciplines such as civil (construction of new buildings, separated rooms, cable trays) or modifications of support systems (extension of battery capacity, replacement of HVAC components).

In 2000, a group of regulatory and safety authorities' experts published a paper to provide a common position on licensing of safety critical software for nuclear reactors. This paper has evolved over the years expanding its guidance to its present 2018 version [15].

5.1.3 Interpretation of Requirements/Wording

In 2019, WNA published the revised "Comparison of Definitions of Key Concepts" [16] based on the claim, that even on the definition and interpretation of key concepts[19] differences exist between regulators and SDOs. The report concludes that after years of harmonization some organizations still rely on different definitions. "The wide variety of terms used for what are essentially the same concepts will make communications between vendors and regulatory agencies difficult" [16]. Early harmonization and common interpretation of the needs and requirements is an essential prerequisite for a successful modernization project.

Next to the identification of requirements for modernization, stakeholders should have a common understanding (interpretation) of them. The use of different terminologies by the stakeholders participating during the project execution, design solutions can introduce different results than what was expected. Interpretation of key concepts forms the basis for the project. This might result from culture or language differences or be driven by history.

For the correct interpretation, it is essential to harmonize the elaborated specific requirements for the system to meet regulatory demands at a very early stage of the project. WNA recommends that a specific exchange meeting be scheduled on the matter and to use the requirement engineering methodology (see Section 5.4.1).

5.1.4 Simplicity in Safety I&C Design

Evolution/further development of I&C hardware and software components (*i.e.* modules) typically intend to provide additional features. These features might be introduced to increase the scope of functionality (*e.g.* for complicated and extensive calculation), self-monitoring features (*e.g.* to reduce or eliminate periodic testing), operational behaviour (*e.g.* system overlapping monitoring and control) or reduction of footprint (increase of signal/function density). I&C modernization projects may also introduce new system interfaces. These additional functionalities and interfaces go hand-in-hand with the increase of complexity.

The introduction of digital I&C provided vendors more flexibility in design solutions. The introduction of digital I&C has also introduced more demands on the verification and validation of the products (software development and hardware integration) and the plant-specific I&C system.

While for operational I&C systems, the complexity of the products is not seen as a crucial issue, regulators and operators have issues regarding trust with "new" digital technology even though the supplier provides qualification certificates and statistical

[19] Key concepts are: Defence-in-Depth, Diversity, Separation, Redundancy, Reliability/ Availability, Spurious Activation and Independence.

data on field operation time. The discussion on the need for diversity (*e.g.* between DiD levels) is directly linked with the discussion on complexity.

The 2018 IAEA Nuclear Energy Series report NP-T-2.11 [13] comments in Section 3.6 on "elimination of unnecessary complexity in I&C" and refers to IAEA SSG-39 [5] stating that "Unnecessary complexity should be avoided in the design of I&C safety systems". Especially for the DiD Level 3 I&C systems (*e.g.* reactor protection system) the main focus should be on "simplicity in design".

The fundamental regulatory challenge posed by "highly-integrated" I&C designs is not one related to technology or design; instead it is a problem of understandability. The overall I&C architecture provides a framework to systematically develop, present, and understand the I&C design base in the necessary context (*i.e.* at the plant level) before attempting to understand the I&C design at the system/technology level.

An I&C system design approach should facilitate the systematic documentation of the 'Why' questions:

- Why do the various I&C functions exist?
- Why are I&C systems scoped the way they are?
- Why are the I&C functions allocated as they are?
- Why do the interfaces between I&C systems exist?

The benefits inherent in a given design can usually be derived from the *why* and not from the *how*. Only the *hazards* can be seen in the *how*. Understanding the *why* and the *how* is critical before understanding the requirements imposed to mitigate *hazards* imposed by the *how*.

Providing the basis for the system engineering decisions that lead to the inclusion of capabilities reflected in the I&C architecture and providing the supporting information related to the regulatory decisions associated with the acceptance of the system architecture would make the regulatory reviews more predictable and efficient.

The discussion of simplicity is by itself complex. Annex C provides some more input to the discussion of the topic. If seen as relevant, a dedicated action could be initiated by DICTF.

5.1.5 Conflicting Requirements: Human-Machine Interface vs Independence

The main control room provides the control room staff with the human-machine interface and related information and equipment, *e.g.* the communication interfaces, which are necessary for the achievement of the plant operational goals [17]. Modern control room concepts for new builds but also for plant modernization favour the usage of multi-visual display units (VDU) and operator support systems (OSS).

In 2019, IAEA published a new Specific Safety Guide SSG-51 on "Human Factors Engineering in the Design of Nuclear Power Plants" [18]. By use of the Document Preparation Profile [19], IAEA stated: "A strong emphasis is being placed on the independence of safety provisions at different levels of the defence in depth. The human intervention on plant remains an aspect that cannot easily be diversified. Hence, human factor engineering which has been carefully considered during the design constitutes a cornerstone of the defence in depth. […] The advances in I&C technology have led to the enhancement of human-machine interface, *e.g.* the use of digital instrumentation and displays." I&C modernization projects may also introduce new alarm and diagnostic message capabilities associated with self-testing features that need to be integrated into the existing plant alarm systems.

The requirements on independence (driven from safety of the plant) and the requirement on human factors (driven from operability of the plant) can appear conflicting. Providing the operator a central platform for monitoring and control of the NPP for all safety and non-safety related systems secures a harmonized and centralized human-machine interface. The plant operator can have a quick and easy overview of the ongoing activities within the plant (process feedback, alarms, trends, *etc.*) and control the plant by use of a few clicks (power increase/decrease, change plant parameter settings, acknowledge system status).

These possibilities of conflicting requirements are linked to the discussion of simplicity/complexity in the previous section. Even if at I&C Layer 3, where different requirements regarding separation and diversity might be specified, it is essential to find the right balance.

5.2 Challenges Related to Facility Configuration Identification

This section deals with the existing or available "as-built" documentation of the NPP.

5.2.1 Quality of As-built Documentation – General

The challenge with incomplete identification of the OEM design requirements is mainly linked to challenges due to incomplete facility configuration identification of the NPP. The engineering life cycle of

20-30 years ago did not require the same scope of documentation as today. This is especially true as the documentation of the overall I&C architecture design and the (detailed) specification of safety I&C function is usually only partially available and may not have been maintained with the plant configuration. It is also the case that modern digital I&C architectures are more complex than previous systems and must be thoroughly documented during the design phase.

This incomplete documentation of the as-built status leads to the situation where, with respect to the I&C Equilibrium, the balance of what "must be confirmed" is typically not given. Carrying out a modernization project without sufficient documentation of the as-built status of the plant can lead to challenges during project execution. The impact of missing facility configuration identification depends on the type of modernization. In order to have a detailed enough picture of the facility to be modernized, the utility is often required to perform a reengineering of its installed systems (that are linked to the SSCs to be modernized).

Some plants in the 1990s, especially in the US, had to go through a design basis reconstitution process because the regulator identified this issue and mandated reconciliation or reconstitution.

5.2.2 Functional Requirement Specification Documentation (As-built)

I&C system safety classification can be recognized as one of the main causes for issues in modernization projects. In NPPs the safety class of a system (and its components) specifies the qualification and quality assurance needed to be demonstrated through the engineering life cycle of the related I&C system. Since the publication of IAEA SSG-30 [6] and IEC 61226 [20], the generic methodology has been changed so that safety classification of an I&C system is now directly derived from the highest safety category of the function to be realized by the I&C system. IAEA SSG-30 in 2014 introduced the relationship between functions and postulated initiating events taking into account the severity of consequences if the function is not performed (see Table 1 of SSG-30 [6]). Following this approach, the first step is to identify, describe and categorize all I&C functions (to be modernized). Such a detailed I&C function specification is typically not in place in older plants. Even for existing plants, regulators might expect current safety classification guidance and a complete set of documentation for modernization projects. More challenges related to I&C Safety Classification are mentioned in the recently revised WNA CORDEL DICTF report "Safety Classification for I&C Systems in Nuclear Power Plants" [21].

Apart from the topic of classification, the scope of the functions to be realized by the system also plays a role. Together with the regulator, it has to be clarified whether there are changes in the design base that may require the installation of new/ additional functions.

5.2.3 Defence-in-Depth and Diversity Concept (As-built)

Beside safety classification, the defence-in-depth and diversity (DiD&D) considerations could also become an issue in I&C modernization projects[20]. Derived from lessons learned but also from application of new (software based) technologies, the general defence-in-depth concept for NPPs has been revised. Depending on the type of modernization, defence-in-depth has to be considered in

[20] depending on the type of modernization – see Chapter 2

combination with the requirements on diversity. I&C functions that have been assigned in the past to one I&C system (due to usage of the same I&C platform) might need to be separated into independent (and diverse) I&C systems. Without a preliminary DiD&D analysis during the feasibility study, the impacts for the modernization scope might be uncertain. The 2018 WNA CORDEL DICTF report on DiD&D [22] gives more information on the challenges related to I&C architecture.

5.2.4 Documentation of Implemented Modifications/ Verification and Validation Documentation (As-built)

Missing documentation from previously performed modifications and verification and validation (V&V) might become another challenge for a modernization project. Through the lifetime of an I&C system, functional improvements and optimizations (minor modifications) are typically implemented over the years. For such modifications, basic design documentation might not have been fully updated accordingly. Missing or incomplete documentation of (minor) modifications leads to disruption of the I&C Equilibrium and might lead to a situation where the upcoming (major) modernization is built upon incorrect basic design data.

Next, the records of the executed V&V activities constitute an important basis for the required V&V actions to be executed during the engineering life cycle of the modernization. Depending on the type of modernization (replacement/ upgrade), tests executed in the past could be repeated in the same or a similar manner. For these projects one main target is to demonstrate the (functional, technological) compatibility between old and modernized systems. Missing V&V documentation makes demonstration of compatibility even more challenging.

Original plant documentation (already in place) might be unreadable or unchangeable, as drawings become degraded over the years or the tools for viewing/editing files or data are no longer supported. For the engineering life cycle, facility configuration documentation should be readable by available tools. From the reengineering standpoint, access to the documentation is mandatory.

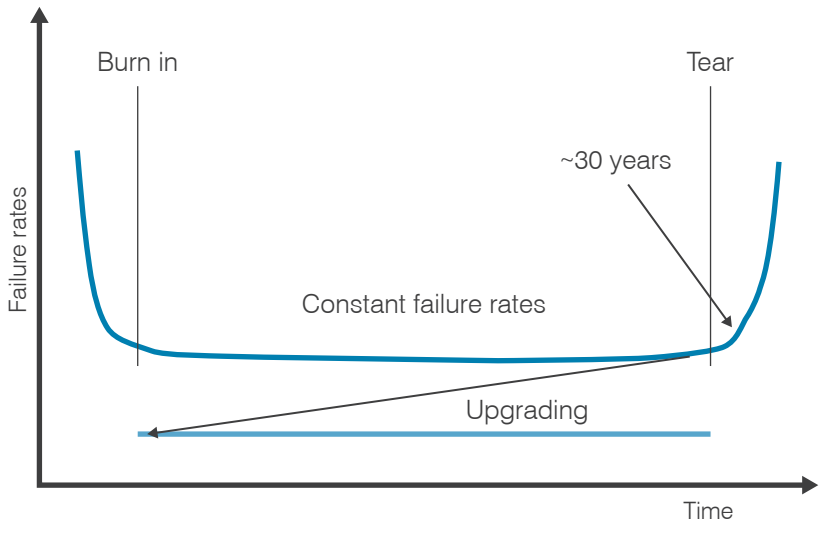


Figure 8. "Bathtub curve" for the service life of components

5.3 Challenges Related to Physical Configuration

This section deals with the "as-built" and "as-modified" status of the installed I&C SSCs at the NPP.

5.3.1 Identification of Installed Inventory

The basis for the I&C life-time management plan (see Annex A) is to have the (detailed) overview of all the components installed in the plant. It requires the complete coverage of all components (regardless of safety class) installed in the plant (including storage), regarding the identification of the related system, location, component type, version, module number, *etc.* To maximize the I&C lifetime, the utility should remain aware of the state of its components (including cables) by periodic inspections, for example. By coupling awareness of the installed components and the information provided by the supplier (spare part availability, failure rates, *etc.*) the utility should have a clear picture to plan for adequate I&C lifetime management. Lack of such data requires the need for reengineering, investigation and preparation of related information as mentioned earlier.

5.3.2 Component Service Life

One of the main questions utilities ask is how long will components be reliably able to function properly (service life). To discuss the service life of components, industry refers to the well-known "bathtub curve" (see Figure 8). Phase one ("burn in" - more frequent failure rate during first startup) and phase two (low/ constant frequent failure rates during operation) may typically be left out of the discussion based on the experiences of the supplier. Apart from the case where the component includes parts affected by wear

(such as capacitors or fans) the third phase of the bathtub curve ("tear" - abrupt increase of failure rate) is more challenging. Depending on the environmental conditions and the treatment during periodic testing/ maintenance, the service life of a component could be much longer than originally stated by the supplier. Each utility should perform its own analysis for its plant, supported by experience from other utilities and the original supplier.

5.3.3 Qualification of Nuclear Safety Components

As in the non-nuclear industry, nuclear utilities are faced with the lack of available spare parts or the feasibility of repairing faulty components. In addition to common issues with non-nuclear industries, nuclear utilities face the challenge of having to meet changing regulatory requirements regarding qualification processes. Depending on the availability of the components, the move from analogue to digital might be necessary, resulting in more extensive work on quality demonstration plus the discussion of common cause failure.

WNA recommends consideration of the availability of qualified components is included in the concept phase. In case components have to be qualified or re-qualified, the planning of the necessary activities should be done at the beginning of the project in order to get all necessary proofs in time.

5.3.4 Reutilization of Existing SSCs

For most types of I&C modernization, only selected SSCs will be replaced. Depending on the scope of modification, the driver and the existing plant configuration segments of the I&C signal chain/I&C Layer may not be included in the modernization, such as the sensors, the I&C rooms, the existing HVAC or power supply. For the reutilization of these SSCs, it is essential to analyze the impact of the intended modernization.

Regarding the lifetime management plan, components not faced with the obsolescence issue or plant improvement needs are out of scope for modernization. As long as these SSCs ensure and demonstrate the required features (accuracy, response time, *etc.*) according to the given plant requirements and the functional task is unchanged, no additional analysis is required. This becomes challenging if the existing use of the component will change. The following examples could lead to this issue:

a) Component classification change (and derived needs on qualification, redundancies, diversifications, *etc.*)

   Example: The functional requirement specification constitutes one of the major input documents for a safety I&C modernization. Section 5.4.3 introduces the potential need for reengineering of the installed I&C functions. As a result, existing functions might be of a higher category than the qualification applied to the components in the past. This could even affect components of the I&C signal chain which were to be kept untouched.

b) Range extension of existing applications (components)

   Example: The installed I&C and supply SSCs were designed for a certain mission/purpose (including margins) during the plant basic design (20-30 years ago). This includes SSCs such as cable trays, penetration assemblies, HVAC for the I&C rooms, fire/ smoke detection, extinguishing systems or communication systems. I&C modernization has typical effects on these SSCs and might require functional extensions or re-use of existing components, such as cable trays. Existing cable trays were engineered and approved according to rules and regulations valid at the time of the erection phase of the plant. Routing of new cables over existing cable trays might require the demonstration of new separation criteria or (intensified) earthquake requirements. Depending on the facility configuration identification (static calculations, construction plans, *etc.*) a re-certification of existing cable runs might not be possible.

c) Intensification of environmental (qualification) requirements

   Example: Based on lessons learned from Fukushima, most regulators revised their environmental requirements such as seismic requirements. Today modernization has to be designed to fulfil these more conservative approaches. Demonstration of structural stability cannot be done by I&C itself. Interdisciplinary calculations need to be executed to provide sufficient information for the regulatory assessment. Depending on the quality of the existing facility configuration identification, additional investigations might be required.

d) Use of spare space/spare resources
   Example: The NPP operator typically requires, in its contracts, sufficient spare space/spare resources for the design of the I&C system(s). Depending on the OEM I&C supplier, capacities are provided by a mixture of reserve zone for new I&C cabinets (including access to cable trays), spare space inside cabinets, unused signal channels on installed modules

or free capacities of memories, processors, communication channels, *etc.* Assignment or application of these reserves without sufficient consideration of possible dependencies with existing functionalities could be the root cause for new failure scenarios, such as overload of processing capacities, failure mode and effect impacts, or loss of functional independence.

e) Interfaces to interconnected systems

   Example: The replacement of a system requires that all interfaces to the still existing systems are carefully managed accordingly. Therefore, it is necessary to check the exact parameters for the signal exchange (structure of the data protocols, electrical signal range, connection type, *etc.*).

5.3.5 Installation Density/Spare Space for New Installation

Even if the OEM provides for spare space in the original plant design, since plant takeover, these areas frequently get used up by plant modifications such as the installation of new systems (*e.g.* plant improvements). The less reserve zone/spare space, the more complicated the modification becomes. Time pressure increases for a modernization project, if the footprint of existing racks, cabinets or even I&C systems are to be reused for the new SSCs. Disposition of sufficient reserve zone/spare space makes it possible to perform preparation activities (in a previous outage or during plant operation). On the other hand, reutilization of the footprint might maximize the reuse of the existing cabling.

It is advisable to create the basis for later modernization already for new builds. This should not be limited exclusively to spare spaces but should, if possible, include concepts for changes to *e.g.* the cabling or the control room.

5.3.6 Characteristics on Change from Analogue to Digital

Retrofits, by use of FFF modules, focus on the 1:1 replacement of the existing inventory faced with the obsolescence issue. This typically provides more advanced technical opportunities such as monitoring and self-test features.

The use of higher packing density of several calculation steps within a single module (such as a Field Programmable Gate Array, FPGA) and the implementation of even a slightly different functional approach could, however, be the cause for new (unexpected) scenarios.

Example: For gradient formation of a differentiator, analogue circuits have a certain delay and damping, whereas new digital modules might overact and issue extremely high gradients at the output. This could cause unexpected behaviour for the plant operator.

5.3.7 Upgrade of Digital I&C System

The intention of an "I&C (digital) system upgrade" (*i.e.* digital-to-digital upgrade) is to provide the operator with an upgrade of existing but outdated digital components/platform to an up-to-date configuration (hardware in combination with software) without replacement of the whole system. While in modernization projects (type 2 to 5 – see Section 2.1), a phased-out I&C platform is replaced with a new and up-to-date one, in upgrade projects, an I&C platform is updated from a previous software and/or hardware generation to an up-to-date version belonging to the same product family. In upgrades, a major part of the existing hardware components, including the wiring, is not affected.

Modern (digital) system platforms need to be partitioned into hardware and software "components". In particular, the life cycles of software components are typically shortened, due to their complexity and continuous improvement. The focus for I&C upgrade projects is concentrated on the demonstration that the upgraded system fulfils the same requirements regarding process and safety. The main challenge for such an upgrade project is to demonstrate the functional compatibility and the correct interaction of the hardware components of different generations together with the new target software version (system software) to ensure technological compatibility without relying on I&C system-specific factory tests (*e.g.* at test field).

Even if most of the safety I&C platform suppliers have a generic programme for lifetime management of their platform(s), each I&C system upgrade introduces possibly new challenges derived from the unique combinations and interactions of components. I&C safety platform development should consider the "downward compatibility" of their modules in its design; that is to say components from the recent production line could be used in system configurations of former settings/module versions (with no or minor modifications). For this reason a supplier might, for example, provide the feature to operate a module in a different mode, the so called "Compatibility Mode" (100% pin and function compatibility) or the "Standard Mode" (new features provided by the new version of the module).

In addition to the application software (I&C functions realized by software means) a digital I&C system consists

of the so called "System Software"[21] which is defined as "operational system software"[22] and "support system software".[23]

Example: A single module type of (digital) I&C system (installed in 1998), *e.g.* communication module, has been phased out for several years. Only a few spare parts are in the component inventory of the operator (no modules in the stock of the supplier). The risk for unavailability of the system increases. Replacement of the whole system (due to one obsolete module) is not an option (*e.g.* remaining lifetime of the plant <15 years). Following the continuous improvement of the safety I&C platform, the original supplier offers the usage of the new module type with the restriction to operate the system with more recent system software.

5.3.8 Plant Dependencies

Each I&C system of a plant assumes a role assigned to it, whether for the safety or for the operation of the plant. The decisive factor here is that, depending on plant state, individual systems are required to be in operation. For this reason, it is important to evaluate each I&C modernization with regard to which of the components may be necessary for the safe operation of the system during the targeted plant outage. Depending on the system architecture (degree of redundancy/ separation of components) and type of function (monitoring, automatic function, *etc.*) this might be solved by temporary or administrative replacement measures.

Example: The I&C system to be modernized includes monitoring and control functions for fuel pool cooling. The required actuators can be operated manually from the control room or locally. The necessary information (temperature) is displayed in the control room. Since the system must also be in operation during replacement of the original system, corresponding temporary replacement measures, such as the establishment of a temporary measurement value acquisition in combination with administrative instructions to the personnel, shall be provided.

5.4 Challenges Related to Work Process

This section deals with the challenges regarding the implementation of activities/work packages and encountered by the stakeholders.

Tools are often already considered as the solution to those challenges. For the implementation of work processes, however, it is necessary to first deal with the proposed conceptual solution. Only in the second step should a tool that best meets the requirements be selected. If necessary, the process (the methodology) should then be adapted to the tool.

5.4.1 Requirements Engineering & Management

Quality assurance work processes (see Section 4.4) have to be developed and followed by the utility and its supplier(s). For the identification of the design requirements a thoroughly planned engineering life cycle is essential. This comprises the quality assurance plan (including the specification of the engineering life cycle) and processes for things such as configuration management and requirements engineering and management. Without using the support of tools (*e.g.* Cradle[24], DOORS[25]), the management of the extensive scope of data and the required documentation is not feasible.

[21] Note this term is used inconsistently in IEC 61513 [9].

[22] Including: application software library, runtime environment, operating system, communication software, i/o drivers, self-supervision functions, *etc.*

[23] Including: engineering tools (such as tools to engineer and generate the application software, graphic editor, code generator, *etc.*), verification and validation tools, tools to design service applications (*e.g.* masks/ scripts), *etc.*

[24] A requirements capture, requirements management and systems engineering tool that delivers stable and reliable requirements management by 3SL (Structured Software Systems Ltd).

[25] Dynamic Object-Oriented Requirements System, an IBM product.

5.4.2 Time Slot(s) for Modernization - Stepwise vs All in One Slot

For many plant modernizations, the time available plays a major role in determining the I&C modernization type. It is advisable to synchronize major I&C modifications at the same time as other modifications in order to minimize plant downtime. The I&C departments should coordinate any need for modernization with the higher-level plant designers at an early stage to secure interdisciplinary synchronization.

Depending on the type of modernization (see Chapter 2), different approaches for the installation in the plant should be assessed. By considering the application of comprehensive V&V measures prior to plant installation (such as analysis, simulations, test bay) consistent with the safety class of the I&C system), modernization types 1, 2 and probably 3 do not need extensive consideration of the implementation time schedule. Such modifications could typically be implemented during normal plant outages.

At least for types 4 (new I&C cabinet implementation) and 5 (new I&C systems implementation), plus consideration of the existing installation density (see Section 5.3.5), the implementation needs to be diligently scheduled by use of the "I&C system – Installation and Commissioning Plan". Every protraction of a plant outage is cost-intensive. In general, the longer the period, the more challenging is the return of investment. Based on recent experiences, a "complete replacement in one outage" for an extensive plant modernization might be reasonable from the overall plant perspective but includes high risks on overall coordination and licensing.

Depending on the scope of modernization (derived from the plant/I&C lifetime management plan – see Annex A), a stepwise installation might be preferred.

> Example: A challenge for a stepwise installation is consideration of the interfaces/ interactions with other SSCs. A temporary modification might be necessary to manage the transition from one modernization step to the next.

A stepwise installation might involve multiple regulatory approvals and typically last several years, which challenges the ability to keep the team united without too many position changes. Each outage should be carefully analysed to determine which activities can be performed as early as possible without affecting the plant operation too much. Planning can be supported by *e.g.* 3D scans of locations, virtual reality or digitalized documentation.

Independent of the type of modernization, insufficient preparation (without consideration of the challenges listed in this section) could be the cause for project delays.

5.4.3 Reengineering/ Reassessment (interdisciplinary)

The scope and type of an I&C modernization project are the main parameters for the level of complexity of the stakeholder's overall work processes (interaction between stakeholders). The replacement of old systems and components is typically focused on a functional 1:1 exchange, for example requiring less support from process and safety disciplines. As for a new implementation (I&C cabinet/I&C system replacement) the utility (and respectively the suppliers) are typically required to assess the impacts for all SSCs and various engineering disciplines interlinked with the modernization scope. This typically includes a reassessment of, for example:

- I&C functional specification (including assignment of the I&C functions to the DiD level and safety category);
- Separation criteria (physical separation regarding rooms/ cable trays, electrical isolation, functional independence and independence of communication);
- Diversity criteria (equipment, design, functional, human, *etc.*);
- Human-machine interface (alarm concept, plant operation, *etc.*);
- IT security (access, cyber control, *etc.*);
- Operation and maintenance (periodic testing, *etc.*);
- Supply systems (electrical power supply, environmental conditions, *etc.*);
- Internal and external hazards (earthquake, fire, missiles, *etc.*).

Depending on the quality and scope of the existing plant documentation (see Section 4.2 - Facility Configuration Identification), comprehensive reengineering might be required.

The more complex the scope, the more interaction (work process) between stakeholders is required. Without close cooperation between the utility and the supplier(s), the work process increases the risk of project execution being inefficient. Efficiency requires a common understanding on how to work jointly including the clear definition of responsibilities.

5.4.4 Systems Engineering 4.0

(Systems) Engineering has been in place as far back as the earliest inventions including the wheel (Engineering 1.0). Since

the introduction of computers (Engineering 2.0) and the application of first 3D modelling tools (Engineering 3.0) the evolution of systems engineering is making enormous advances. Engineering 4.0 now focuses on the overall integration of participating stakeholders [WL 2].

Recently many companies have installed or planned to implement a (Model Based) Systems Engineering (SE) approach. SE is not a new phenomenon. It has been practised for decades, for example by merging different technologies or safety-related missions that cannot be investigated using a prototype.

The increased level of complexity and interaction of various different disciplines and stakeholders through the whole life cycle of a nuclear power plant modification require a holistic and systematic approach to achieve "right the first time". The systems engineer ensures that the outcome satisfies requirements, on the first attempt and at the right time. Systems engineering has established itself in fields where complicated connections prevail or where critical safety aspects have an influence and human lives are in jeopardy. Nothing is left to chance and nothing should go wrong upon introduction.

INCOSE [23] has defined Systems Engineering as:

"Systems engineering is an interdisciplinary approach and should methodically enable the development of systems. SE focuses on a holistic and cooperative understanding of stakeholder requirements, the discovery of potential solutions and the documentation of requirements, as well as the synthesizing, verification, validation and development of solutions. Meanwhile, the entire problem is analysed, from conceptualization to system development. Systems engineering provides suitable methods, processes and best practices for this purpose."

As discussed in Section 5.2.2, a traditional functional requirements specification can be recognized as one of the main causes for issues. More important is the discipline overlapping the engineering process. Independent of the project stakeholders, it is essential to have a common understanding on work processes, data transfers (input/output) and voting procedures. Systems Engineering 4.0 provides the philosophy and the tools to do this.

Late design modifications (identified during the installation/commissioning phase) could be cost-intensive, and may lead to project delays or even loss of confidence in the overall system. Lessons learned from past modernizations and new build projects have shown that, most frequently, late design modifications have been requested as a consequence of functional requirements findings. Process and safety experts are most of the time sufficiently involved in the overall engineering process (including verification and validation measures). With the use of SE 4.0 philosophy plus the application of a specific engineering tool chain (to secure digital consistency of data) the request for "right the first time" should be secured.

The installation and implementation of new systems engineering methodologies requires an extensive change of working methods for involved stakeholders. Especially for stakeholders cooperating for the first time, sufficient time should be spent to harmonize engineering life cycle activities.

In 2019, IAEA initiated a new work item: "Adoption of Systems Engineering Principles for Nuclear Power Plant Instrumentation & Control". The objective of this activity is to provide guiding principles for applying a structured approach to systems engineering for I&C systems in order to promote the uses of systems engineering when developing I&C systems.

5.4.5 Configuration Management

Configuration Management (CM) is a mandatory prerequisite for each modernization project. This includes information on the installed SSCs (physical configuration) and the revision of the valid system documentation (facility documentation). CM furthermore oversees configuration change control, status accounting and release management. All stakeholders have to support the CM work process during the entire engineering life cycle. Coordination between stakeholders is of utmost importance.

5.4.6 Staggered Licensing Process and Risk Reduction

For the implementation of the I&C life-time management plan, the I&C department of the utility must provide figures on the estimated cost of plant modernization to its owners (economic drivers). Therefore during the call for tenders, suppliers are typically asked to submit estimated costs for turnkey solutions meeting all stakeholder design requirements. At this stage for safety related I&C, many uncertainties remain from a licensing perspective, so it is challenging for suppliers to identify them all in one solution when offering the best price (with only a few exceptions).

It is especially true for safety I&C modernizations of type 4 or 5 (new I&C cabinet/I&C systems implementation) that engineering efforts and project risks are difficult to estimate in detail at the

early stages. Imprecise design requirements, disagreements, vague understanding of licensing issues, inadequate bid preparation and calculations on a short notice lead to a point where during contract negotiation each partner intends to specify exceptions or to transfer licensing risks. Considerable time is lost in negotiations and leads to more pressure on the overall time schedule. Some regulators require first the submission of a feasibility study on the generic modernization concept in order to get approval to move to the next stage. A bottom-up approach on such a study would simplify and reflect more precisely the scope of modernization, the technical description and the economic risks for all contract partners (see Figure 6).

During project execution, it is advisable to consider approval steps between operator and supplier as well as between regulator and operator that build on each other during the project life cycle typically following the approval process of the regulator.

5.4.7 Overall Demonstration of V&V Coverage

IAEA SSG-39 [5] requires:

"2.69. The overall I&C, each I&C system and each I&C component should be verified to confirm that all of the requirements (both functional requirements and non-functional requirements) have been met, and to determine whether any undesirable behaviour exists (see paras 2.128–2.142). The requirements defining the overall I&C, each I&C system and each I&C component should be validated to confirm that they are fulfilled as intended."

Depending on the type of modernization, separate but interdependent life cycles for the overall I&C architecture and one or more per individual I&C system are required. For each, a life cycle demonstration of the correct implementation/realization of the design requirements needs to be performed. Derived from the safety class of the SSCs, the scope and type of V&V activities differ. Since many stakeholders contribute to a life cycle, the overall demonstration of the V&V coverage becomes challenging for the overall supplier.

Without installation of an encompassing capturing and data management of the input requirements, including the identification (documentation) of the intended and (successful) executed V&V actions, an overall demonstration becomes quite complex.

> Example: For a new build project, very intensive discussions on the "I&C test concept" have been performed. The operator requested information on the general organization and strategy of testing the I&C, including I&C system test, I&C architecture tests and I&C functions tests which have to be performed prior to first commercial operation. The sooner within the life cycle requirements this can be sufficiently demonstrated, the lower the probability of missing design faults later (*e.g.* during the commissioning phase). Without a common agreement between involved stakeholders, additional V&V actions might be required during late design phases leading to project delays and cost increases.

5.5 Challenges Related to Staff Skills (Knowledge Management)

This section deals with challenges on the knowledge skill set requirements with which nuclear stakeholders are confronted.

5.5.1 Know-how Transfer

The challenge of adequate staff knowledge and skill is not only linked to the application of new technologies or engineering methodologies. In fact the most critical aspect is the loss of knowledge on the existing 20 years and older NPP designs. This includes the whole range of I&C related activities from the generic overall OEM plant design up to specific knowledge of dedicated module behaviors.

> Example: For I&C modernization type 2 (FFF module replacement), it is essential to have the knowledge and skill related to the real technical behavior of the installed single modules. Depending on (analogue) module characteristics, these properties might not be documented in the official descriptions of the module but are known by the original designers (*i.e.* tribal knowledge). Missing or wrong interpretation of documentation could lead to incorrect modernization and substantial additional expenses.

5.5.2 Staff Reduction/ Replacement

Faced with economic challenges, NPP stakeholders are asked to reduce the number of their employees. Experts retiring or leaving might not have been adequately replaced. To build up knowledge from I&C junior design engineers up to I&C senior chief engineers takes at least 5-8 years (or even longer). For the transfer of knowledge from a leaving senior chief engineer to an appointed successor (*e.g.* chief engineer) at least 6 months are needed. Increased pressure on project execution might force the stakeholder to spend less time on education and knowledge transfer which might lead to troubles in the long run.

Whilst experts used to work for different departments and working areas during their career in the past (*e.g.* installation, commissioning, basic design, analysis), today employees might be much more focused on their dedicated working area without gaining knowledge about interfacing activities. Based on the type and scope of modernization, the level of complexity requires having architect engineers covering the whole engineering scope per discipline. Failing to adequately fill these positions can be the cause for challenges during project execution.

5.5.3 Team Integration

Following the idea of System Engineering (see Section 5.4.4), close interaction and efficient cooperation between the stakeholders is essential for a successful project. Of course, to secure integrity of each stakeholder, independent teams and quality assurance methods are required to be installed. Besides the timely involvement of experts, team integration plays a decisive role.

Experiences from the past have demonstrated that plant operator and supplier should work as one entity to support transparency on selected design solutions and better understand the needs and constraints of others. If possible, the composition of the team should be local and follow the project life cycle needs (supplier site: basic design and test bay/plant site: installation and commissioning). This close cooperation demands flexibility form each side to serve the overall project goal.

6 Summarizing Remarks

One of the main objectives of the CORDEL Working Group and its Task Forces is to promote international standardization of design approaches. Through this report on I&C modernization, CORDEL DICTF intends to examine the topic afresh through analysis of the current status and challenges linked to elements of the I&C equilibrium.

CORDEL DICTF provides the industry (utilities and suppliers) with a forum to exchange and highlight their experiences. These are used to inform reports on safety classification, on defence-in-depth and diversity and now on I&C modernization. The goal of these reports has been to inform and start an exchange/ discussion with regulators and SDOs on the subject.

Many of the stakeholders involved in these projects have had a variety of positive and negative experiences in the field of I&C modernization. Learning from each other would do much to improve safety and drive economies.

This report builds upon the findings of a technical workshop: "Current Status and Difficulties of I&C Modernization", organized from 29 to 31 October 2019 by CORDEL DICTF in cooperation with IAEA.

The objectives of the workshop were to:

- Share international experience, lessons learned and best practices through presentations and discussions on I&C modernization at nuclear power plants;
- Improve understanding of the main challenges in I&C modernization and how they can be overcome;
- Identify opportunities for harmonized approaches in I&C modernization;
- Share insights and obtain input from workshop participants on the development of this paper; and
- Support the IAEA and World Nuclear Association in defining future activities for I&C applications.

CORDEL DICTF will continue to work on the topic of I&C modernization, collecting and analysing lessons learned from industry (operators/ suppliers), examining issues in greater depth, and developing a checklist for modernization projects. It intends to maintain a close cooperation with the IAEA and other organizations such as IEC and IEEE.

References

[1] IAEA Safety Glossary, *Terminology Used in Nuclear Safety and Radiation Protection*, International Atomic Energy Agency (2018)

[2] IAEA TECDOC-1016, *Modernization of instrumentation and control in nuclear power plants*, International Atomic Energy Agency (1998)

[3] IAEA SSR-2/1, *Safety of Nuclear Power Plants: Design*, International Atomic Energy Agency (2016)

[4] IAEA SSR-2/2, *Safety of Nuclear Power Plants: Commissioning and Operation*, International Atomic Energy Agency (2011)

[5] IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, International Atomic Energy Agency (2016)

[6] IAEA SSG-30, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*, International Atomic Energy Agency (2014)

[7] IAEA NS-G-2.3, *Modifications to Nuclear Power Plants*, International Atomic Energy Agency (2001)

[8] IAEA NP-T-1.13, *Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants*, International Atomic Energy Agency (2015)

[9] IEC 61513, *Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems*, International Electrotechnical Commission (2011)

[10] IEC TR 62096, *Nuclear Power Plants – Instrumentation and Control Important to Safety – Guidance for the Decision on Modernization*, International Electrotechnical Commission (2009)

[11] IAEA SRS No. 65, *Application of Configuration Management in Nuclear Power Plants*, International Atomic Energy Agency (2010)

[12] IAEA TECDOC-1335, *Configuration Management in Nuclear Power Plants*, IAEA (2003)

[13] IAEA NP-T-2.11, *Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants*, International Atomic Energy Agency (2018)

[14] IAEA NP-T-3.12, *Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants*, International Atomic Energy Agency (2011)

[15] *Licensing of Safety Critical Software for Nuclear Reactors - Common Position of International Nuclear Regulators and Authorised Technical Support Organisations*, Bel V, BfE, CNSC, CSN, ISTec, KAERI, KINS, ONR, SSM, STUK, NSC (Regulator Task Force on Safety Critical Software) (2018)

[16] *Safety Classification for I&C Systems in Nuclear Power Plants: Comparison of Definitions of Key Concepts – Revision 2019*, World Nuclear Association (2019)

[17] IEC 60964, *Nuclear Power Plants – Control Rooms – Design,* International Electrotechnical Commission (2009)

[18] IAEA SSG-51, *Human Factors Engineering in the Design of Nuclear Power Plants*, International Atomic Energy Agency (2019)

[19] IAEA DPP, *Document Preparation Profile for New Safety Guide DS492 – Human Factors Engineering in Nuclear Power Plants*, International Atomic Energy Agency (2014)

[20] IEC 61226, *Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions*, International Electrotechnical Commission (2009)[26]

[21] *Safety Classification for I&C Systems in Nuclear Power Plants, Current Status and Difficulties – Revision 2020*, World Nuclear Association (2020)

[22] *Defence-in-Depth and Diversity: Challenges Related to I&C Architecture*, World Nuclear Association (2018)

[23] INCOSE-TP-2003-002-03, *Systems Engineering Handbook, A Guide for System Life Cycle Processes and Activities*, International Council on System Engineering (2006)

Weblinks

[WL 1] Wikipedia - *Single source of truth:* https://en.wikipedia.org/wiki/Single_source_of_truth

[WL 2] The SOLIDWORKS Blog - *Engineering 4.0:* https://blogs.solidworks.com/solidworksblog/2014/10/engineering-4-0.html

[26] Currently being revised.

Annex A | Generic Approaches for I&C Modernization

Introduction

This annex provides a brief overview to the general factors to be considered for each modernization project.

A-1. Drivers for I&C Modernization

It is essential to first identify all the main parties involved in the modernization of NPPs and to understand their roles and responsibilities. The stakeholders are:

- National authorities – regulators;
- Power supply operators – utilities;
- Standards development organizations (SDOs)/international organizations;
- System suppliers – vendors;
- Public (consumer);
- National states
- Neighbouring countries.

The main factors justifying modernization are driven by safety and/or economic considerations requested by the utilities themselves or by the regulators (see below). Utilities and regulators have the general duty to secure the provision of (clean) energy with minimal risks to the public and the environment.

The ***national regulators*** are mandated by the state to assure that the utilities construct and operate their power plants in accordance with national regulations. Regulators are required to continuously consider lessons learned from operating experience (worldwide) and address concerns from experts and the public to keep the operating (and design) requirements current. This leads to the publication of revised or new national regulations or safety guides. In addition, for some states the regulator is obligated to perform systematic safety reassessments, termed periodic safety review (PSR), to assess the cumulative effects of plant ageing and plant modifications, operating experience, technical developments and site aspects. Resolving findings (deficiencies) is the responsibility of the operator within a given time frame.

The ***utilities*** need to consider economic factors as well. For operating power plants, the costs for energy production can be optimized by:

- reducing maintenance work (and subsequently maintenance employees);
- increasing average power output (*e.g.* duration of operating time in relation to outage time, increase of maximum power output by plant optimization, and reduction of downtimes on component faults);
- savings in fuel (optimization of fuel) and reduction of operating/ administration costs (*e.g.* reduced spare parts inventory, decrease of operating and maintenance team).

To ensure uninterrupted plant operation especially in light of plant license extensions, modernization might be required. From an economic perspective the utility has to compare the cost to postpone modernization with the return on investment to decide whether to modernize or to stop operation[1]. Nevertheless, the utility has the responsibility to secure safe operation of the plant and to minimize risks to the environment (safety aspect).

[1] Usually I&C modernization does not generate "direct" cost savings. The benefits will come from lifetime extension, power upgrades, reduction of maintenance costs, *etc.*

SDOs and international organisations such as IEC and IEEE, as well as IAEA and OECD/NEA, have the mission to establish international harmonized requirements and guidelines for the construction (and operation) of power plants. The regulations and safety guidelines of the national regulators are typically based on the work of the SDOs. Depending on the organization, the SDOs' work is done by nominated experts of regulators, utilities and vendors. In addition to SDOs, international organizations, such as WANO, WNA, NEI, or EPRI, have the same vision to support the harmonization and standardization of safety criteria worldwide. The papers, guidelines, and codes & standards published by the SDOs and these other organizations are on a lower hierarchical level than the national regulations/laws.

System suppliers (vendors) offer solutions (systems/products) to satisfy the utility's needs (sponsor) and regulator's requirements (authority) whilst competing against other vendors (locally, regionally or worldwide). The mission of vendors is to profit their companies by offering competitive engineering and maintenance services and/or products. The supplier provides experts for the engineering (design, validation and verification (V&V)), manufacturing, and commissioning of the systems for the power plant. Based on a utility's request, the vendor delivers a solution in line with the utility's economic (and safety) expectations by considering the applied regulations (safety). Obtaining the regulator's approval of the solution is the responsibility of the utility with support from the vendor. The vendor's experts typically have significant knowledge of the safety, process and system design of the power plant under consideration with regards to the regulations and codes & standards to be applied.

The public demands a reliable supply of low cost electricity with minimal risk to the health and safety of the public and the environment. Long-standing loss of electricity (blackout) would have a huge impact on daily life as the modern world is significantly dependent on electricity. On the other hand, worst-case scenarios, such as Fukushima or Chernobyl, have made the public aware that safety is very important in the field of electricity production by nuclear power plants. Depending on the culture, media, the level of information received from other sources (such as scientists, experts, educators, authorities in the field), the willingness of the people to consider a certain percentage of remaining risk differs. The national regulators have the duty to address this fear.

The decision to undertake I&C modernization is typically based upon a mixture of different safety and economic drivers such as (see also IEC TR 62096 [A-1]):

Safety drivers:

- recommendations of a safety review (*e.g.* periodic safety review);
- changes in licensing requirements (*e.g.* management of new failure scenarios);
- implementation of new regulatory requirements (*e.g.* defence-in-depth and diversity concepts/separation constraints);
- lessons learned from plant related incidents/occurrences in other plants (worldwide);
- deficiencies revealed by ongoing inspections;
- reduction of human errors.

Economic drivers:

- obsolescence of installed equipment;
- end of product's life cycle;
- ageing - due to: chemical effects; drying out of electrolytic capacitors; cables and other components made from organic material; mechanical effects such as wear; seizure that leads to failure of mechanisms in relays, *etc.*;
- competence of personnel - decreasing availability of skilled workers for maintenance and operation of obsolete I&C systems;
- incomplete or inaccurate as-built documentation'
- compatibility - issues with interfacing connections or protocols for modernized equipment;
- operational - issues with:
  - new operator requirements – functional upgrades;
  - necessity to perform flexible operation – ability of nuclear power plants to adjust core thermal power to match electrical demand and control frequency of the electrical system;
  - fuel management changes – different fuel design, configuration and enrichment, refuelling management;
  - power upgrade.
- reduction of maintenance costs – lower limitation of spare part inventories/ reduction of manual periodic testing.

The age of the power plant and competition (open electricity market competing with low oil/gas prices and subsidies for new energy sources *e.g.* wind, solar) lead to a situation in which utilities are under much more economic pressure to optimize production costs. In addition to market pressure, the safety drivers from regulators (resulting from lessons learned/postulated new scenarios) lead to more extensive work on safety of the construction (including modernization) and operation of nuclear power plants. Considering these factors requires a forward-looking and conscious plant lifetime management.

A-2. Lifetime Management

I&C modernization is mainly driven by the need to manage obsolescence of the installed equipment and to secure overall plant availability for the future. I&C equipment, like other hardware, has a lifetime determined by physical, chemical and environmental conditions and can also be subject to hardware fault/damage. I&C equipment should not become a factor impacting plant availability, therefore a lifetime management program for the I&C equipment is essential.

Based on the lifetime management strategy, the plant operator should have an early and good overview of upcoming modernization priorities. Some operators have considered this approach already, that is to say the plant operator has performed a continuous modernization program, and some others have procrastinated on this matter and are only focused on maintenance (*e.g.* replacement of faulty modules). Both approaches fit the purpose to secure availability for the plant but with different consequences when the time comes to perform a plant-wide I&C modernization project.

Regarding plant lifetime management, the utility will rely on its strategic plan(s) to guide the progression from the present state to the future vision for the I&C structures, systems and components (SSCs). This future vision is identified by the overall plant lifetime management plan deduced from the overall plant goals, objectives and commitments. This plan works as the central planning tool for electrical, mechanical, civil or I&C disciplines.

The management of the overall lifetime management plan needs to include identifying the status of the installed SSCs (per discipline). The plant I&C architecture integrates the I&C SSCs and their interfaces with the rest of the NPP taking into consideration the plant's defence-in-depth approach. Driven by the need to manage the configuration of the plant, each plant component must be identified. Using existing plant information (*e.g.* service lifetime, needed preventive maintenance, availability of replacement parts, spare parts stock, increased failure rate, ageing analysis, *etc.*) preliminary data is available to assess the need for modernization. The results of this assessment are the input for the overall plant lifetime management plan needed to schedule, calculate and prioritize future modernization tasks. In addition, anticipated new regulatory requirements (*e.g.* driven by safety review/changed licensing requirements) are to be considered during the periodic revision of the lifetime management plan.

All these factors provide the "roadmap for modification" that will drive the initiation of a specific modernization project. Figure 1 provides an example of the workflow for a modification (*i.e.* modernization project) in a nuclear power plant based on an overall plant lifetime management plan (from IAEA-TECDOC-1335 [A-2]). As indicated by IEC TR 62096 [A-1] there is a strong need to start with feasibility studies for generic and technical issues.

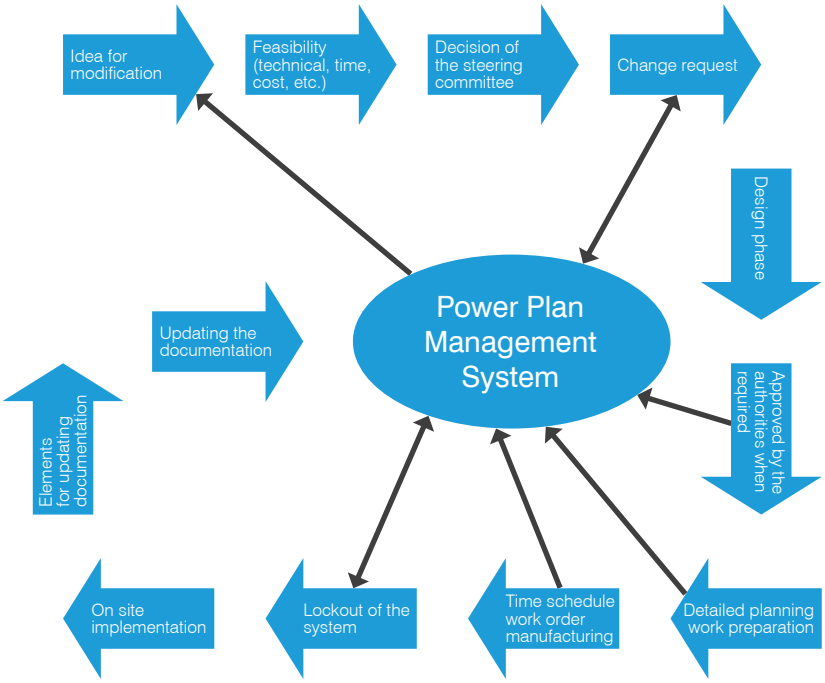


Figure 1. Example of workflow for a modification in a nuclear power plant (IAEA TECDOC-1335 [A-2])

References

[A-1] IEC TR 62096, *Nuclear power plants – Instrumentation and control important to safety – Guidance for the decision on modernization*, International Electrotechnical Commission (2009)

[A-2] IAEA TECDOC-1335, Configuration management in nuclear power plants, International Atomic Energy Agency (2003)

Annex B | Collection of Codes & Standards and Guidelines on I&C Modernization

Introduction

This annex provides information on the normative references to be taken into account for the modernization of safety I&C system(s) in nuclear power plants. The normative references are supplemented by complementary/informative references such as TECDOCs (IAEA), Technical Reports (IEC) or Design Guides (EPRI) – see Table 4 at the end of this annex. The annex gives a short overview of the available documents, their intention and quotes the most important, extracted, content.

For each I&C modernization project the scope of normative reference(s) shall be established between all stakeholders during the initiation phase.

B-1 IAEA

1.1. IAEA – Specific Safety Requirements

1.1.1. IAEA SSR 2/1: NPP Design Safety [B-1]

IAEA SSR 2/1 represents the top level of the international normative references for I&C. It is focused on the safety design of (existing and new) NPPs[1] and identifies requirements to be considered for new plant design, not for modernization projects.

Requirement 31 - Ageing management:

> *The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.*

Requirement 62

> *Instrumentation and control systems for items important to safety at the nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed.*

1.1.2. IAEA SSR 2/2: NPP Operation Safety [B-2]

IAEA SSR 2/2 is focused on the commissioning and operation of NPPs. It specifies the need to perform lifetime management of the overall plant including its systems, structures and components.

Requirement 14: Ageing management

> *The operating organization shall ensure that an effective ageing management programme is implemented to ensure that required safety functions of systems, structures and components are fulfilled over the entire operating lifetime of the plant.*

[1] The requirements established in the IAEA Safety Standards might not be fully met at some existing facilities that were built to earlier standards. The way in which IAEA Safety Standards are to be applied to such facilities is a decision for individual States

Requirement 16: Programme for long term operation

Where applicable, the operating organization shall establish and implement a comprehensive programme for ensuring the long term safe operation of the plant beyond a time-frame established in the licence conditions, design limits, safety standards and/or regulations.

1.2. IAEA – Specific Safety Guides

1.2.1. IAEA SSG-39 [B-3]

The SSG-39 could be seen as the top-level document for engineering or I&C for NPPs. Section 1.14 identifies the scope/type of projects it covers as follows:

The guidance applies to the design of I&C systems for new plants, to modifications of existing plants and to the modernization of the I&C of existing plants.

The chapter on "Modifications" provides more information:

2.158. The design of upgrades and modifications to I&C should consider:

- *Limitations resulting from the physical characteristics of the installed plant that effectively restrict the design options for I&C systems;*
- *The possible need to maintain consistency between the design of replacement equipment and existing I&C equipment in order to, for example, reduce the complexity of the overall operator interface and maintenance tasks of the plant;*
- *Practical considerations with respect to the equipment or technology that is commercially available and the prospects for securing support of such equipment and technology by manufacturers or third parties for the installed lifetime of the equipment;*
- *The need to update existing design documentation.*[2]

2.159. When an I&C system is modified or is part of an upgrade, the level of rigour to be applied in justifying and executing the change should be established beforehand.

2.160. The level of rigour should be based upon the role and function of the affected systems in ensuring the safety of the nuclear power plant, in association with the existing systems that will remain in operation after the work. This also applies to changes to software tools.

2.161. Development of the modification or upgrade of I&C systems should follow a specified life cycle.

2.162. The complexity of the life cycle process needed for modifications is related to the complexity and safety significance of the modification.

2.163. The life cycle for even the simplest changes should include at least the phases of the individual system life cycle shown in Fig. 2, including verification and validation after each I&C modification.

[2] The design documentation for older systems might be incomplete or inaccurate. Consequently major modifications to or replacement of such systems might require some degree of 'reverse engineering' to recreate the original design base and specifications.

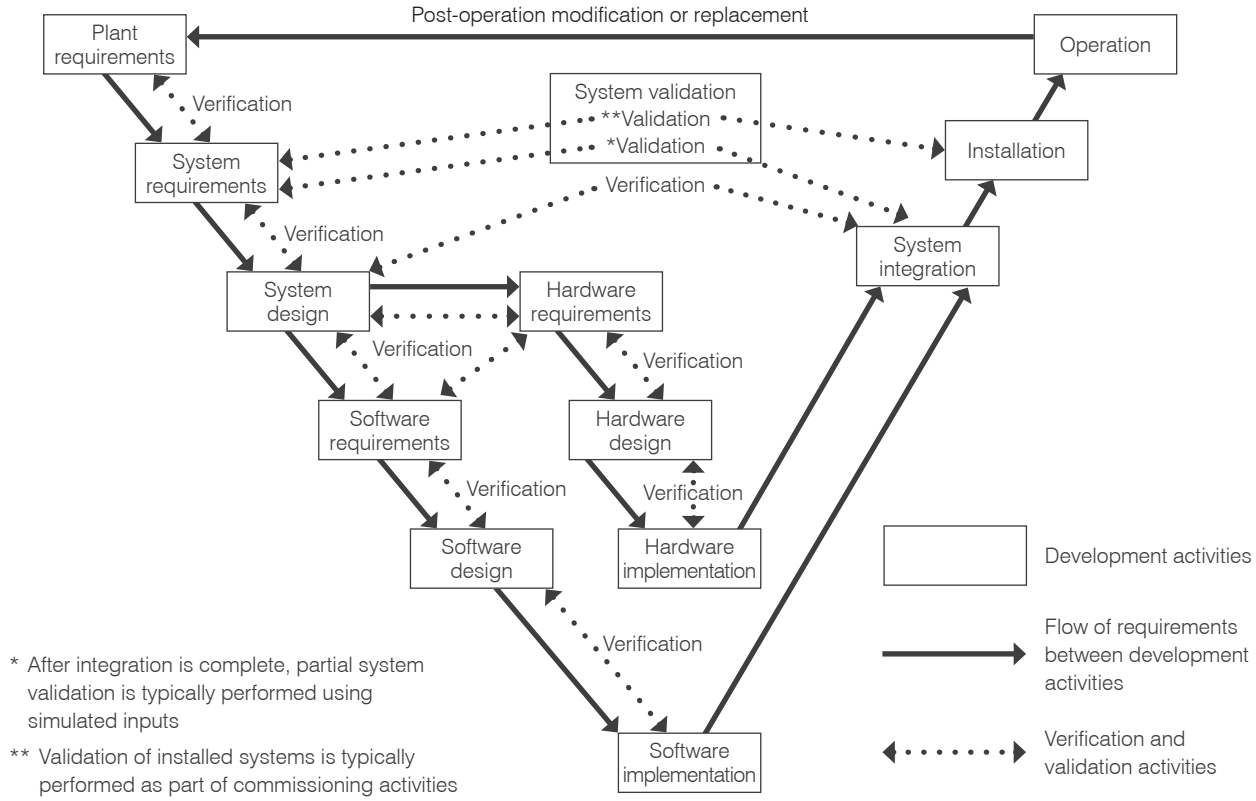


Figure 1. Typical relationship between I&C life cycle process and verification and validation activities (IAEA SSG-39 Fig. 2 [B-3])

2.164. Interim configurations of the human-machine interface that represent a transition between new and existing I&C might need further analysis from a human factors engineering perspective to accommodate the use of temporary equipment or procedures. Enhancements to the interface with the operator might lead to an increase in errors by operations personnel and maintenance personnel for some time after the change. In some cases modifications to training might be necessary.

2.165. When an I&C system is replaced, consideration should be given to running the new I&C system in parallel with the old system for a probationary period, i.e. until sufficient confidence has been gained in the adequacy of the new system. The equivalent of parallel operation might be possible by installing new redundant equipment in one train at a time.

2.166. When considering the parallel operation of I&C systems, the disadvantages of operational problems and complexity should be weighed against the gain in confidence, and the risks should be evaluated.

2.167. The consequences of an update or change in software tools between the time of initial development and the modification may be significant and should be assessed for its impact (for example, a compiler upgrade could invalidate previous results of analysis or verification concerning the adequacy of the compiler).

1.3. IAEA – Series information

IAEA Safety Series reports such as Nuclear Safety Guide (NS-G), Nuclear Power Objectives and TECDOCs have the objective to provide guidance and recommendations on controlling activities. The following reports have been published in the past 20 years by IAEA on the subject of I&C modernization.

1.3.1. NS-G-2.3 – Modification to Nuclear Power Plants (Safety Guide – 2001) [B-4]

The objective of IAEA NS-G-2.3 is to provide guidance and recommendations on controlling activities relating to modification at NPPs in order to reduce risk and to ensure that the configuration of the plant is at all times under control and that the modified configuration conforms to the approved basis for granting a nuclear power plant operating licence (refer to I&C equilibrium).

It is not an I&C-specific guide but deals with the modification of structures, systems and components.

In Section 2 it specifies the generic process for modifications in NPPs (see Figure 2).

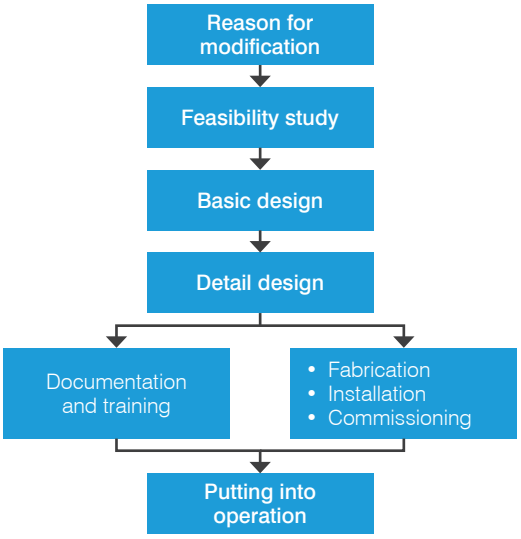


Figure 2. Basic process for modification in a nuclear power plant (simplified – based on IAEA NS-G-2.3 [B-4])

The safety guide identifies the following reasons for modifications:

- Rectify weaknesses in components;
- Failures discovered during operation, inspection or maintenance;
- Prevent faults or reduce their frequency;
- Improve maintainability;
- Incorporate a non-identical replacement of a plant component;
- Take account of changes in safety standards.

NS-G-2.3 identifies three categories of modifications depending on the scope, the driver and recommendations for the setup of the modernization.

Category 1:

Scope: Significant effect on radiological risk or may involve an alteration of the principles and conclusions on which the design and the licensing of the plant were based.

Driver: Changes in the set of design basis accidents/alterations in technical solutions meeting the safety goals/changes in operating rules.

Setup: Analysis + Prior approval + Amendment to operating licence or new licence.

Category 2:

Scope: Changes in safety-related items or systems and in operational approaches and/or procedures, and usually necessitating an update of the safety analysis report or other licensing documents.

Driver: Minor influence on safety and no significant alteration to the principles on which plant licensing has been based. No changes to conclusions in the licensing documents.

Setup: Contact regulatory body in accordance with established procedures.

Category 3:

Scope: Minor modifications (no consequences for safety/items classified as not important to safety and not mentioned in the licensing documents. Design/implementation error could not lead to significant increase in risk).

Driver: Not identified.

Setup: Reported to regulatory body only if required.

The principles for managing modifications are the same for all categories, but in each step of the modification process the categorization of the modifications determines the depth and breadth of the safety review and the regulatory control which should be applied.

1.3.2. SSG-48 - Ageing Management and Programme for Long Term Operation [B-5]

Objective:

This Safety Guide provides guidance for operating organizations on implementing and improving ageing management and on developing a programme for safe long term operation for nuclear power plants, which, among other aspects, takes due account of ageing management.

The Safety Guide may also be used by the regulatory body in preparing regulatory requirements, codes and standards, and in verifying effective ageing management in nuclear power plants.

This Safety Guide focuses mainly on managing the physical ageing of SSCs within the scope of ageing management ('in-scope SSCs'). It also provides recommendations on safety aspects of managing technological obsolescence and recommendations on the programme for safe long term operation of nuclear power plants with emphasis on ageing management related activities.

Effective ageing management throughout the lifetime of SSCs requires the use of a systematic approach to managing the effects of ageing that provides a framework for coordinating all activities relating to the understanding, prevention, detection, monitoring and mitigation of ageing effects on the plant's structures and components.

This approach is illustrated in Figure 3[3], which is an adaptation of Deming's 'plan–do–check–act' cycle to the ageing management of SSCs.

[3] Refer to Figure 1 in the main report

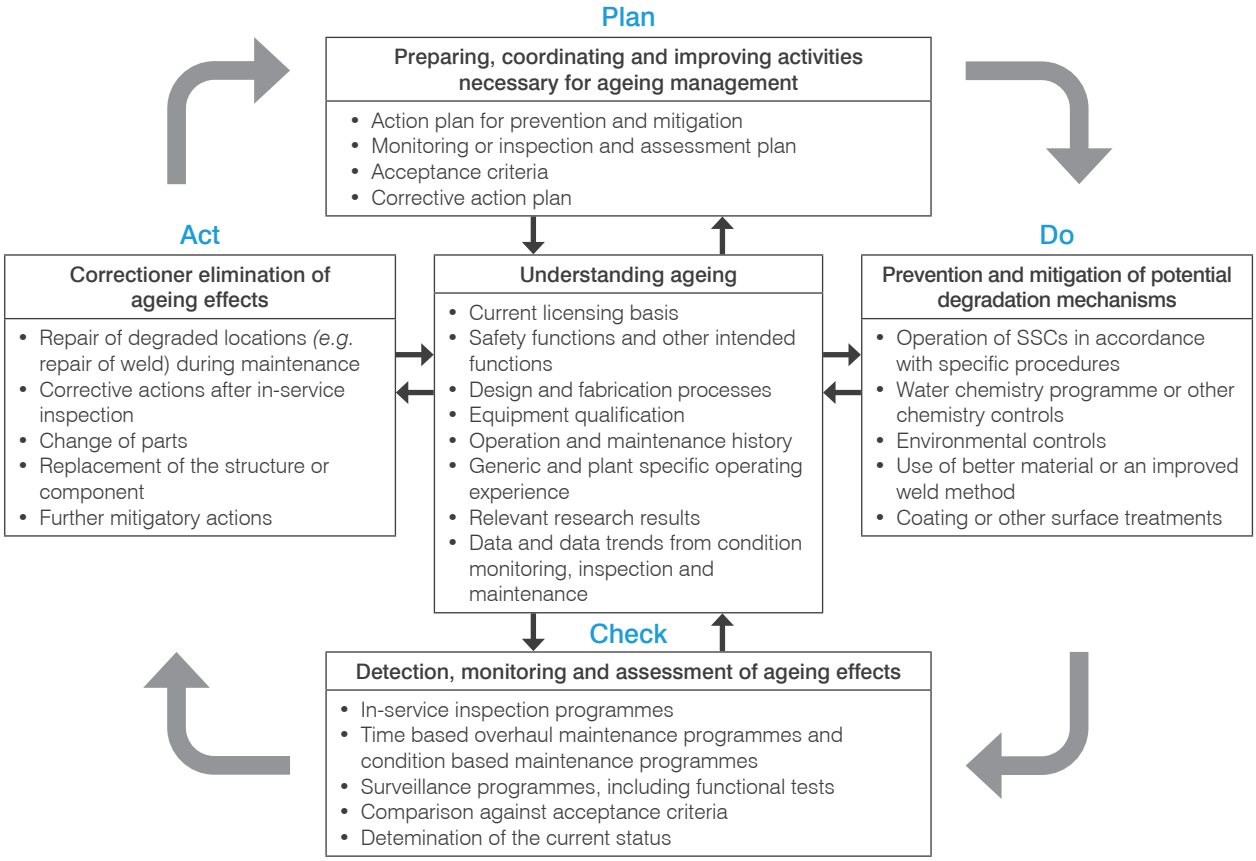


Figure 3. Systematic approach to ageing management (IAEA SSG-48 –Figure 1 [B-5])

Table 1 in SSG-48 identifies several types of obsolescence including their related manifestation, consequences and management approaches.

Table 1 Types of obsolescence (IAEA SSG-48 Table 1 [B-5])

Subject of obsolescence	Manifestation	Consequences	Management
Technology	Lack of spare parts and technical support Lack of suppliers Lack of industrial capabilities	Declining plant performance and safety due to increasing failure rates and decreasing reliability	Systematic identification of useful service life and anticipated obsolescence of SSCs Provision of spare parts for planned service life and timely replacement of parts Long term agreements with suppliers Development of equivalent structures or components
Regulations, codes and standards	Deviations from current regulations, codes and standards for structures, components and software Design weaknesses (*e.g.* in equipment qualification, separation, diversity or capabilities for severe accident management)	Plant safety level below current regulations, codes and standards (*e.g.* weaknesses in defence in depth or higher risk of core damage (frequency))	Systematic reassessment of plant safety against current regulations, codes and standards (*e.g.* through periodic safety review) and appropriate upgrading, back fitting or modernization
Knowledge	Knowledge of current regulations, codes and standards and technology relevant to SSCs not kept current	Opportunities to enhance plant safety missed	Continuous updating of knowledge and improvement of its application

1.3.3. NP-T-1.4 - Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants (2009) [B-6]

Objective:

This document will explain a process for planning and conducting a modernization project based on the experience gained from projects which have already been completed. In addition, numerous issues and areas requiring special consideration are identified. It is the intent of the authors to present an outline of a process which is relevant for I&C modernization projects in all countries, and to identify significant issues which have proven to be important based on their collective experience.

1.3.4. TECDOC-1500 – Guidelines for Upgrade and Modernization of Nuclear Power Pant Training Simulators (2006) [B-7]

Objective:

The objective of this report is to provide practical guidance on the various technical and project management aspects of the upgrading and modernization of nuclear power plant (NPP) full scope control room simulators.

1.3.5. TECDOC-1389 - Managing Modernization of Nuclear Power Plants Instrumentation and Control Systems (2004) [B-8]

Objective:

The overall objective of this report is to facilitate the cost effective implementation of new (most likely software-based) I&C systems in nuclear power plants. This is necessary to address obsolescence issues, to introduce new beneficial functionality, and to improve overall performance of the plant and staff. Non-nuclear industries have, in general, already made the change in technology from analog (hard-wired) to digital (software-based). The same technology, and accompanying techniques to implement it, is being introduced now into more and more nuclear power plants for both safety and safety-relevant applications. Effective management experience and lessons learned from these other industries need to be collected and used as appropriate for more cost effective modernization of I&C systems in nuclear power plants. However, the nuclear industry has some unique requirements that must also be addressed cost effectively.

To successfully implement new I&C systems, it is necessary that the safe operation of such systems in nuclear power plants has to be proven during the licensing process in order to gain the acceptance of licensing authorities, as well as acceptance in the plant itself. Effective management to meet the required high quality of the assessment of the nuclear power plant I&C systems within acceptable costs is needed.

1.3.6. TECDOC-1402 - Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance (2004) [B-9]

Objective:

This TECDOC will use the existing body of information and knowledge from the worldwide nuclear power industry to build a case for the role of I&C in plant performance improvements in terms of both plant safety and plant economy. It will then provide recommendations as to what can be done to prevent I&C ageing and obsolescence from affecting the safe and economical performance of NPPs.

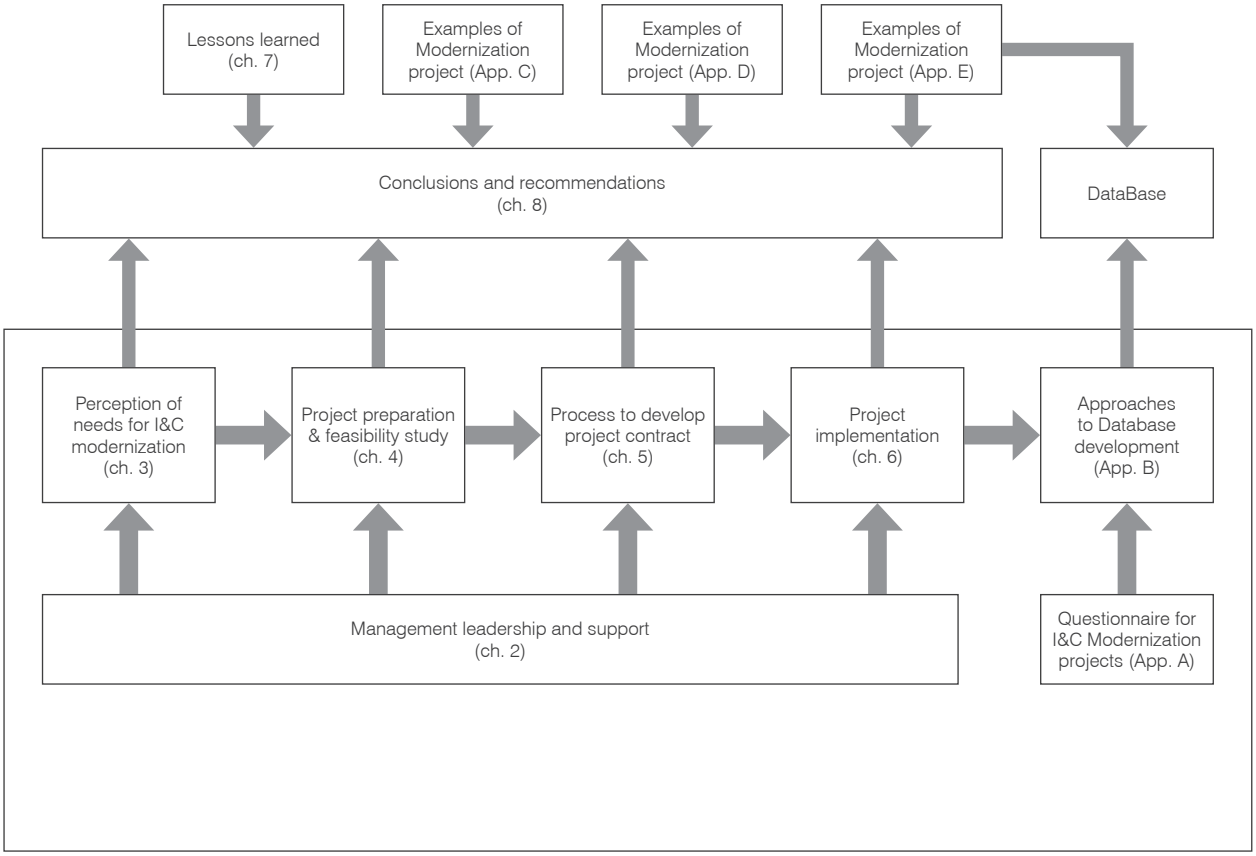


Figure 4. Basic relation structure of the main text (IAEA TECDOC-1389 Figure 2 [B-8])

1.3.7. TECDOC-1066 - Specification of Requirements for Upgrades Using Digital Instrument and Control System (1999) [B-10]

Objective:

- *The to provide guidance, without prejudicing the working practices of the readers and users, for subjects which the specifications of requirements for digital I&C systems should include at different phases of the life cycle of a project;*

objectives of this report are:

- *to provide guidance, without prejudicing the working practices of the readers and users, for subjects which the specifications of requirements for digital I&C systems should include at different phases of the lifecycle of a project;*
- *to outline, and later in the report to define more clearly, a methodology which minimises the risk of omitting important requirements from the specifications for digital I&C refits and upgrades;*
- *to ensure all elements of requirements which are needed in the various specifications are identified, so that they take account of significant influencing factors such as safety and utility preferences.*

1.3.8. TECDOC-1016 - Modernization of Instrumentation and Control in Nuclear Power Plants (1998) [B-11]

Objective:

This report is designed to identify methodologies, guidelines, processes, concerns, and good practices to help in the modernization of I&C systems of NPPs. It has been developed by the contributors from their experience in identifying the need for modernization and in the performance of actual modernization planning and implementation projects. The methodologies, guidelines, processes, and good practices identified in this report have been developed for and tested on actual modernization activities. It is expected that the user of this report will be able to gain valuable information and experience that will allow future modernization projects to be performed more cost-effectively. This same information and experience will allow the modernized systems and components to be implemented in a manner that will improve productivity, reduce costs, and enhance safety.

1.3.9. NSS33-T – Computer Security of Instrumentation and Control Systems at Nuclear Facilities [B-12]

Objective:

Chapter “Modification of I&C system”

4.206. The application of computer security measures to legacy I&C systems at an existing nuclear facility is not always straightforward. For example, the following difficulties may arise:

- *Alteration of the legacy I&C architecture may not be possible without affecting the deterministic behavior of the legacy I&C systems.*
- *Existing technologies used for program or data storage, interfaces, or communication may not support modification.*
- *Existing facility structures and layout may not allow for sufficient physical protection measures.*
- *Contemporary technical control measures that provide security monitoring functions may not be compatible with the technologies implemented within legacy I&C systems.*

4.207. During the modernization of a nuclear facility that involves the replacement of legacy I&C systems with modern I&C systems, the operator should consider the possibility that legacy interfaces with the original facility systems and other systems may need to be maintained and that new vulnerabilities and weaknesses may be introduced owing to the new technology or design.

4.208. Modifications of I&C systems change the system or its documentation. These changes may be categorized as follows:

- *Changes or enhancements (corrective or adaptive);*
- *Migration (i.e. the movement of a system to a new operational environment);*
- *Replacement (i.e. the withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system).*

4.209. I&C system modifications may be derived from requirements or specified to correct errors (corrective), to adapt to a changed operating environment (adaptive), or to respond to additional operator requests or enhancements.

4.210. When modifications to an I&C system are made, an assessment of the security of the modified I&C system should be included, for example, by updating the system CSRM.

4.211. Computer security should be considered as part of the change management process. This includes changes to software and hardware for I&C systems.

4.212. To ensure that vulnerabilities have not been introduced into the facility environment by modifications, the operator should assess proposed I&C system changes including their impact on the computer security programme and existing I&C system security, evaluate anomalies that are discovered during operation, assess migration needs and assess modifications made, including validation and verification activities.

4.213. Computer security measures should be assessed as described in paras 4.206–4.212 above, and should be revised to reflect computer security requirements derived from the modification process, as appropriate.

4.214. During modification, existing I&C system computer security requirements should remain in force unless those requirements are to be changed as part of the modification activity.

4.215. Configuration management for computer security measures should be in place to prevent the introduction of unauthorized software to I&C systems.

4.216. When migrating systems, the operator should verify that the migrated systems meet the computer security requirements for the I&C system.

4.217. Artefacts from development, installation and testing should be removed from the system and its configuration files prior to placing in service for operation.

4.218. Modifications to I&C systems should be treated as development processes and should be verified and validated.

4.219. All modifications to the I&C system and its components, including software, hardware and system configurations, should account for potential security vulnerabilities and threats that may occur not only during the execution of these activities but also as a result of the modifications.

4.220. Many digital assets and associated components, including removable storage media, have the ability to retain digital data when removed from a system. This digital data may include preprogrammed logic or residual system data such as sensor readings, control signals, analytical data and network traffic. These data may be extractable from the discarded components.

4.221. Administrative and technical control measures should be in place to ensure that remnant data on discarded components cannot be used to support the development of a computer exploit. The components should be destroyed or the data should be securely removed, unless residual data on components to be discarded have been evaluated to show that the data do not pose a risk of security compromise.

4.222. For modifications involving the replacement of I&C systems, the operator should conduct activities such as data cleansing, disk destruction or complete overwrite to ensure data cannot be recovered from the replaced I&C system upon removal from service.

B-2 IEC Subcommittee 45A (SC45A) - Instrumentation, Control And Electrical Power Systems Of Nuclear Facilities

Next to IAEA, IEC SC45A represents the main international standard design organization providing requirements for engineering or I&C systems (including I&C modernization). IEC is organized by levels (Level 1 to 4). Level 1 documents provide general requirements for I&C systems. Level 2 provides standards related to categorization of functions, classification of systems, separation of systems, defence against common cause failure, *etc.* and should be seen together with Level 1 as a consistent set of documents. At the third level, IEC SC45A standards are not directly referenced to Level 1. They are related to specific equipment, technical methods or specific activities and can be used on their own. The Level 4 standard series corresponds to technical reports which are not normative.

> Note: The WG A10 produces and maintains standards and reports dealing with the modernization of I&C systems for nuclear power plants. This includes the replacement and upgrading of I&C systems due to obsolescence, ageing, plant life extension activities and other economically, technically, or safety driven motivating factors. Standards covering issues related to the modernization of nuclear power plant I&C systems, such as the management of ageing, are also included in the scope of WG A10.

Enclosed information on the main IEC documents concerning I&C modernization is provided as follows.

2.1. IEC 61513 - General Requirements for Systems (IEC Level 1) [B-12]

IEC 61513 is the first level IEC SC45A document tackling the issue of general requirements for systems. It is the entry point of the IEC SC45A standard series regarding I&C safety systems.

According to section 1.2 (Application: new and pre-existing plants):

> *This standard applies to the I&C of new nuclear power plants as well as to I&C up-grading or back-fitting of existing plants.*
>
> *For existing plants, only a subset of requirements is applicable and this subset should be identified at the beginning of any project.*

Section 5.2.3.1 discusses the assumptions concerning categorisation of functions and classification of systems. The related note stipulates:

> *The normative references for categorisation of functions may vary between countries and deviate from the reference of this standard (IEC 61226). A specific situation may also arise when applying this standard to existing plants where new categorization requirements are valid only for the parts in the scope of a modernization project. In such cases, a specific analysis may be required to identify the minimum requirements per system class.*

Derived from Section 1.2, the scope of IEC 61513 application should be specified during the initial phase of the I&C modernization project.

2.2. IEC 60880 - Software Aspects for Computer-Based Systems Performing Category A Functions (IEC Level 2) [B-13]

IEC 60880 identifies the software-related activities to be executed in the frame of the safety life cycle for computer based systems of Safety Class 1. Modifications in the frame of IEC 60880 are focused on the change of software components/executable code of Safety Class 1 systems initiated for example by changes to functional requirements, software environment, hardware or anomalies found during testing or operation. The more specific requirements on software have to be considered in the overall process execution according to IEC 61513[4].

2.3. IEC 60709 - Separation (IEC Level 2) [B-14]

IEC 60709 establishes requirements for physical and electrical separation as one means to provide independence between the functions performed in those systems and equipment.

Section 5.4 focuses on modernization of existing nuclear power plants.

> *5.4 Separation issues at existing plants*
>
> *5.4.1 General*
>
> *The separation of I&C and electrical systems important to safety in existing nuclear power plants is often incomplete because SSCs that had initially no safety classification may need to be classified as important to safety and because design standards have changed. When upgrading existing plants, the potential consequences of not following this document in all aspects due to practical considerations should be justified against the added safety gained through the upgrade taken as a whole.*
>
> *5.4.2 Criteria*
>
> *Separation issues shall be particularly addressed in the implementation strategy of the plant upgrades. Issues which shall be considered include:*
>
> – *separation in intermediate configurations when new I&C and/or electrical systems are installed through a phased programme;*
> – *identification of subsystems, which can be separated without the need for intermediate interfaces;*
> – *suitability of the existing separation to the new I&C and/or electrical technology (mainly sensitivity of digital I&C to EMI, power semiconductors, special temperature requirements and susceptibility to radiation);*
> – *cable routing limits and an evaluation of the needs coming from new technologies for special cable trays, e.g. for fibre optic cables, bus cables and requirements for separation.*

Guidance for the decision on upgrading and modernisation of I&C can be found in IEC 62096.

[4] IEC 62138 - Software for I&C systems, supporting Category B and C functions, is organized regarding modernization in the same approach as IEC 60880.

2.4. IEC 60964 – Control rooms - Design (IEC Level 2) [B-15]

IEC 60964 provides functional design requirements to be used in the design of the main control room of a nuclear power plant to meet operational and safety requirements. It also provides functional interface requirements which relate to control room staffing, operating procedures, and the training programmes which, together with the human-machine interface, constitute the control room system.

This standard is intended for application to new control rooms whose conceptual design is initiated after the publication of this standard. The recommendations of the standard may be used for refits, upgrades and modifications.

No specific requirements on I&C modernization are provided.

2.5. IEC 62645 – Requirements for Security Programmes for Computer-Based System (IEC Level 2) [B-16]

IEC 62645 establishes requirements and provides guidance for the development and management of effective security programmes for I&C computer-based systems for NPPs. The primary objective of this standard is to define adequate programmatic measures for the prevention of, detection of and reaction to malicious acts by digital means (cyber-attacks) on I&C CB&HPD[5] systems.

This standard is applied to all NPP I&C systems throughout the life cycles of these systems. It may also be applicable to other types of nuclear facilities.

No specific requirements on I&C modernization are provided.

2.6. IEC 62566 – Instrumentation and Control Important to Safety – Development of HDL-programmed Integrated Circuits for Systems Performing Category A Functions (IEC Level 2) [B-17]

IEC 62566 provides requirements for achieving highly reliable HDL-programmed devices (HPD), for use in I&C systems of nuclear power plants performing safety functions of Category A as defined by IEC 61226. The programming of HPDs relies on hardware description languages (HDL) and related software tools.

Regarding the modification process and documentation, IEC 62566 requests to comply with requirements of IEC 61513 (6.2.8 and 6.4.7), IEC 60987:2007 (Clause 12) and IEC 60880:2006 (Clause 11).

2.7. IEC/TR 62096 - Guidance for the Decision on Modernization (IEC Level 4) [B-18]

IEC/TR 62096 is intended to support owners of a nuclear power plant in the decision-making process and in the preparation for partial or complete modernization of I&C. For this, it provides a summary of the motivating factors for I&C modernization, the principal options for the elaboration of different scenarios for I&C modernization, the technical and economic criteria for the selection of a long term I&C strategy, as well as the principal aspects to be taken into account for a detailed technical feasibility study. The structure of IEC 62096 is shown in Figure 5.

[5] CB&HPD - computer-based systems and integrating Hardware Description Language Programmed Devices (HPD)

This new edition includes the following significant technical changes with respect to the previous edition:

- update on references, taking into account standards published since the previous edition;
- update on the terminology;
- incorporation of several clarifications proposed by National Committees.

In addition, this report contains detailed recommendations and practical advice for:

- the technical evaluation of the actual status of the I&C systems;
- the content of the I&C system requirement specification and for the project management following the guidance given in IAEA TECDOC 1016 [B-11] and 1066 [B-10];
- considerations on modernization strategy.

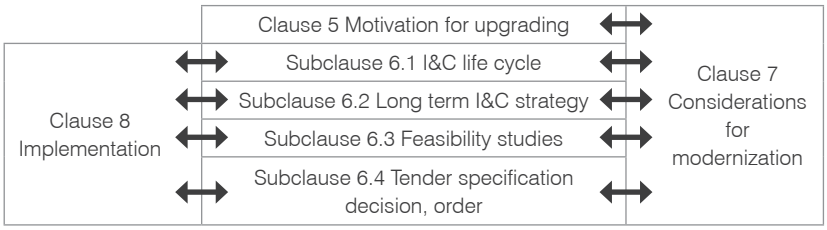


Figure 5. IEC 62096 structure (IEC 62096 Figure 1 [B-18])

IEC 62096 is used as the main reference for this Digital Instrumentation and Control Task Force (DICTF) paper as it has the same intention. Therefore the DICTF paper will focus on new lessons learned in the recent years and link to IEC 62096 for subjects already described therein. The DICTF paper could be seen as a continuation of IEC 62096.

B-3 MDEP Digital I&C Working Group (DICWG)

The Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group (DICWG) common position papers were focused on new reactor design and no requirements were derived from the recent DICWG papers.

Since the transmission to OECD NEA Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC), the scope is extended to plant operation and maintenance (including modernization). DICTF expects increased the collaboration on I&C modernization with WGDIC in the future.

B-4 EPRI – Electrical Power Research Institute

This guide applies Systems Engineering as the foundation to conduct a facility change that adds or modifies digital technologies, whether it's a new plant design, major analog to digital facility change, or a minor update to a software module in an installed digital system.

4.1. Digital Instrumentation and Control Design Guide (2014) [B-19]

The design control elements of the basic engineering change/modification processes for existing plants are typically based on regulations, standards and guidance (e.g., ANSI N45.2.11) that do not specifically address digital design issues. The unique aspects of digital design, especially software elements, often are covered by processes that are not well integrated into the overall plant design change process. This guideline addresses the need to improve the degree to which the digital design process is integrated within a general plant modification process and it addresses digital I&C engineering activities, issues, topics, tasks and deliverables throughout the life cycle of a digital I&C system.

This guideline provides supplemental guidance for implementing design control in plant modifications involving digital I&C equipment and systems. The intended audience for this guidance is owner/operator design engineers and project managers involved in digital I&C modification activities, or their A/E service providers who may be assigned such responsibilities on the behalf of the owner/operator.

This guideline is intended to complement existing policies and procedures used by owner/operators in controlling engineering changes to their facilities.

4.2. Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments (2014) [B-20]

The objective of this report is to provide a set of principles, approaches and guidelines that can be used in developing overall I&C architectures that:

- *Help ensure plant safety while also meeting other competing design constraints related to plant simplicity, reliability, operability and maintainability*
- *Reflect good engineering practice for I&C architecture design*
- *Have a high likelihood of gaining approval from multiple international regulatory bodies.*

The intent is that the guidance can be used by utilities and suppliers working on design and licensing of I&C architectures for new builds and for upgrades to operating plants.

4.3. Instrumentation and Control Strategies for Plant-Wide and Fleet-Wide Cost Reduction (2007) [B-21]

This guideline provides material useful for several audiences. For executives and plant managers, it concisely explains the risks, benefits and issues associated with I&C modernization, and provides tools by which the most suitable approach can be selected. Key decisions are identified, along with who should make them and what is their impact. Plant-wide or company-wide issues, such as existing organization and culture, are highlighted so that they can be factored into the decision, or modified if a new direction is desired.

For I&C department managers and project managers, the guideline identifies changes in planning or execution that can achieve better and cheaper results. It also explains techniques for understanding costs, benefits and risks so that project prioritization and phasing can be done in a more effective manner.

For technical staff, endpoint visions provide prototypical examples of functional requirements for aggressive and resource-constrained approaches, as well as architectural examples that show how each vision can be implemented using commercial technology.

The EPRI document describes four basic I&C options, as shown in Table 3 below.

Table 3 The Four Basic I&C Options (EPRI 1015087 Table 2-1 [B-21])

Option	Productivity Improvement	Initial Investment	Long Term Maintenance	Plant Risks	Project Risks
Aggressive Strategy	High	Low	Med	High	High
Resource-Constrained Strategy	Med	Med	Med	Low	Med
Tactical Upgrades	Low	Low	High	Med	Med
Maintain of Replace Legacy Components	None	None	Very high	Very high	Very low

4.4. Guideline for Performing Defence-in-Depth and Diversity Assessments for Digital Upgrades (2004) [B-22]

This guideline is particularly significant in that it provides a practical approach for the difficult issues on D3 (Defence-in-Depth and Diversity) evaluation and PRA modelling for software-based equipment.

This document provides guidance to support utilities in performing defence-in-depth and diversity (D3) evaluations associated with digital upgrades that affect plant instrumentation and control (I&C) systems. For some digital upgrades, a D3 evaluation is performed to examine potential vulnerability to software or other digital system failures that could simultaneously affect multiple trains or systems. Such failures are referred to in this report as digital common cause failures (digital CCFs). The focus of a D3 evaluation is on digital CCFs that could degrade plant safety. Postulated digital CCFs could compromise the redundancy built into safety systems, or impact defence-in-depth currently provided through the availability of independent protection, control and monitoring systems.

4.5. Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification (2015) [B-23]

Nuclear power plant operators face a significant challenge designing and implementing modifications to control rooms and related human-system interfaces (HSIs) while replacing or updating instrumentation and controls (I&C) to use more modern digital technology. Owner/operators pursuing new builds will be working with a vendor on design and licensing of control rooms and HSIs that already employ largely digital systems, and then will take responsibility for maintaining the design and licensing bases as modifications are made after they begin operation.

This report provides guidance on planning, specifying, designing, implementing, operating, maintaining, and training for modifications to control rooms and related facilities, and making effective use of digital I&C systems and HSIs. Guidance is also provided on planning for new build HSI design and licensing efforts. This report also presents detailed information and guidelines on technologies such as information display systems, soft controls, alarms, automation, computerized procedures, and handheld and other portable devices.

4.6. Advanced Nuclear Technology: Guidance and Methodologies for Managing Digital Instrumentation and Control Obsolescence (2014) [B-24]

New nuclear plant technology will rely heavily, if not exclusively, on digital equipment; and the industry is increasingly migrating to digital-based instrumentation and control (I&C) systems in the existing plant base. Obsolescence of digital I&C equipment is an inevitable part of plant technology life cycle for new and already operating plants. Developing an overall strategic plan can mitigate some of the risks associated with obsolescence. Moreover, when developed as part of an overall life cycle management plan (LCMP), a strategic obsolescence management approach can identify steps that can be taken at early stages of the technology life cycle to cope proactively with the obsolescence of equipment.

Users of this guideline can integrate obsolescence management holistically into a Lifecycle Management Plan. By using the methodologies for identifying and mitigating the risks associated with digital I&C obsolescence, the user or plant owner/operator can proactively manage obsolescence throughout the equipment lifecycle. The ample descriptions of available approaches to strategic planning and the worksheets provided for digital systems distinguish this guideline from the many other resources available for managing digital I&C obsolescence.

4.7. Instrumentation and Control, Human System Interface, and Information Technology Requirements Project Plan for Nuclear Power Plant Long-Term Operation (2010) [B-25]

Nuclear power plant owners are looking to extend the operating life of their plants to 80 years and potentially longer. Instrumentation and control, human system interface, and information technologies have changed drastically since the plants were built and will change even more drastically before the plants reach the end of their operating life. A project plan to develop requirements for these technologies is defined here. These requirements will enable plants to better identify future solutions that will fulfill plant needs.

This report can be used as a guideline to develop a plan that demonstrates a clear, achievable, cost-effective path for defining flexible functional requirements for control room and underlying I&C/IT infrastructure, architecture, and associated capabilities, and that will support plants throughout their extended operating life - even as technologies change.

B-5 IEEE – Institute Of Electrical And Electronics Engineers

5.1. IEEE Std 1205 - IEEE Guide for Assessing, Monitoring, and Mitigating Aging Effects on Class 1E Equipment Used in Nuclear Power Generating Stations [B-26]

IEEE Std 1205 provides guidelines for assessing, monitoring, and mitigating aging degradation effects on Class 1E equipment used in nuclear power generating stations. This guide also includes informative annexes on aging mechanisms, environmental monitoring, condition monitoring, aging program essential attributes, and example assessments for five types of equipment (including electric cable).

The purpose of this guide is to supplement existing IEEE nuclear standards in assessing aging degradation effects. The methods described herein can be used to identify the performance capability of Class 1E equipment beyond its qualified life.

B-6 INL – Idaho National Laboratory

6.1. INL/EXT-14-33129 - Advanced Instrumentation, Information, and Control Systems Technologies: Digital Technology Business Case Methodology Guide (2014) [B-27]

The purpose of the Business Case Methodology (BCM) is to provide a structure for building the business case for adopting pilot project technologies in a manner that captures the total organizational benefits that can be derived from the improved work methods. This includes the direct benefit to the targeted work process, efficiencies gained in related work processes, and avoided costs through the improvement of work quality and reduction of human error.

Specifically, the BCM highlights key questions to ask and guides the utility through, as well as identifies where in the process to employ, the Business Case Methodology Workbook (BCMW) for benefits/cost savings identification. The approach enables collaboration between the Instrumentation, Information, and Control Pathway and utility partners in applying new technologies across multiple nuclear power plant (NPP) organizations and their respective work activities, wherever there is opportunity to derive benefit. In this manner, the BCM drives an "economy of scale" that maximizes the value of the technologies relative to the implementation cost.

The BCM leverages the fact that, in spite of what seems to be a wide and disparate array of work activities among an NPP's operational and support organizations, the work activities themselves are largely composed of common tasks. For example, whether the work activities are in Operations, Chemistry, Radiation Protection, or even Security, they have in common such tasks as pre-job briefs, use of procedures, correct component identification, emergent conditions requiring work package alteration, etc. It is at this task level that the technologies are applied, and therefore the benefits of the technologies can be realized across as many plant activities as can be identified to employ these tasks. In this manner, a much more comprehensive business case can be derived that greatly increases the benefit/cost ratio. This has the added benefit of driving consistency across the NPP organizations, which is a fundamental principle of successful NPP operational and safety management.

B-7 NRC – Nuclear Regulatory Commission

7.1. Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (2016) [B-28]

The NRC staff has developed a strategy to modernize the NRC's regulatory infrastructure to enhance the agency's capability to determine whether there is reasonable assurance of safety and security in digital I&C systems for nuclear facilities. The objective is to provide a process that is timely, efficient and effective, and provides a consistent and predictable regulatory process for NRC staff and stakeholders. In developing the strategy, the NRC staff considered the current regulatory infrastructure, ongoing regulatory activities, and stakeholder input to identify near- and long-term strategies. The NRC staff also followed the high-level principles provided by the Commission in SRM-SECY-15-0106 as listed below:

1. *The plan should include the establishment of a senior management SC to oversee resolution of digital I&C regulatory challenges.*

2. *Any new or revised requirements addressed in the action plan should be performance-based rather than prescriptive.*
3. *Digital I&C safety requirements should be technology neutral; however, guidance should be tailored if necessary. The same requirements should apply to operating and new reactors.*
4. *Guidance should focus on acceptable approaches to complying with requirements and may include specific technology focused provisions. If only one approach is acceptable to the NRC staff to ensure safety based on current understanding, and this approach is appropriately technology-neutral and performance-based, then it should be included in a requirement rather than in guidance.*
5. *NRC requirements and guidance should not pose an unnecessary impediment to advancement in nuclear applications of digital technology.*

The current regulatory process provides reasonable assurance of safety and security through the NRC staff's review and approval of license amendments for specific digital I&C systems and evaluation of new reactor applications that fully incorporate highly integrated digital technologies. However, the timeliness, efficiency, and predictability of the licensing and oversight processes can be improved.

To accomplish these improvements, the NRC staff, in coordination with stakeholders, established an integrated action plan (IAP) (Enclosure 1). The IAP consists of Modernization Plans (MPs) for three key topics: common cause failure (CCF), changes under 10 CFR 50.59 "Changes, tests and experiments," and commercial grade dedication of digital equipment under 10 CFR Part 21. These topics will have the greatest impact, in the near-term, in addressing regulatory challenges and improving timeliness, efficiency, and effectiveness. Successful implementation in these areas is needed to provide near-term regulatory clarity and the necessary confidence on the part of licensees to perform digital I&C upgrades. As part of MP #4A in the IAP, the NRC staff will prioritize and implement the complete set of regulatory activities, including building upon those in the first three MPs.

The longer-term goal, as outlined in MP #4B, is to then evaluate and implement the next steps for continued improvement of the NRC's digital I&C regulatory infrastructure. The infrastructure improvements will result in a state where the nuclear power industry can use current and future digital technology efficiently, assuring safety and security with less uncertainty in the regulatory process, and minimizing the dependence on judgment by utilizing performance-based technical criteria that can be applied consistently across different technologies. The NRC staff will review and modify the current regulatory structure to be more performance based and flexible by using new methods in the most effective way and updating the regulatory and guidance structure to acknowledge changes in the technology, the way it is developed and how it is used. The NRC staff will evaluate the results of implementation of the near-term activities and, with continued stakeholder interaction will develop a performance based, technology-neutral regulatory infrastructure that will anticipate the evolution and future development of digital I&C technology as it is applied to nuclear technologies.

Overview

Table 4. Overview of I&C codes & standards/guidelines related to I&C modernization

Codes & Standards/Guidelines	Normative	Informative
IAEA *IAEA - Specific Safety Requirements*		
IAEA SSR 2/1: NPP Design Safety	X	
IAEA SSR 2/2: NPP Operation Safety	X	
IAEA - Specific Safety Guides		
IAEA SSG-39	X	
IAEA NS-G-2.3	X	
IAEA SSG-48[6]	X	
IAEA - Series information		
NS-G-2.3 - Modification to Nuclear Power Plants (Safety Guide) (2001)		X
NP-T-1.13 – Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants (2015)		X
NP-T-1.4 - Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants (2009)		X
TECDOC-1500 – Guidelines for Upgrade and Modernization of Nuclear Power Plant Training Simulators (2006)		X
TECDOC-1389 - Managing Modernization of Nuclear Power Plants Instrumentation and Control Systems (2004)		X
TECDOC-1402 - Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance (2004)		X
TECDOC-1066 - Specification of Requirements for Upgrades Using Digital Instrument and Control System (1999)		X
TECDOC-1016 - Modernization of Instrumentation and Control in Nuclear Power Plants (1998)		X
IEC SC45A		
IEC 61513 - General Requirements for Systems (IEC Level 1)	X	
IEC 60880 - Software Aspects for Computer-Based Systems Performing Category A Functions (IEC Level 2)	X	
IEC 60709 - Separation (IEC Level 2)	X	
IEC 60964 – Control Rooms - Design (IEC Level 2)	X	
IEC 62645 – Requirements for Security Programmes for Computer-Based System (IEC Level 2)	X	
IEC 62566 – Instrumentation and Control Important to Safety – Development of HDL-programmed Integrated Circuits for Systems Performing Category A Functions (IEC Level 2)	X	
IEC/TR 62096 - Guidance for the Decision on Modernization (IEC Level 4)		X

[6] not specific to I&C

Codes & Standards/Guidelines	Normative	Informative
OECD MDEP DICWG		
EPRI - Electrical Power Research Institute		
Digital Instrumentation and Control Design Guide (2014)		X
Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments (2014)		X
Instrumentation and Control Strategies for Plant-Wide and Fleet-Wide Cost Reduction (2007)		X
Guideline for Performing Defence-in-Depth and Diversity Assessments for Digital Upgrades (2004)		X
Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification (2015)		X
Advanced Nuclear Technology: Guidance and Methodologies for Managing Digital Instrumentation and Control Obsolescence (2014)		X
Instrumentation and Control, Human System Interface, and Information Technology Requirements Project Plan for Nuclear Power Plant Long-Term Operation (2010)		X
IEEE - Institute of Electrical and Electronics Engineers		
IEEE STD 1205 - IEEE Guide for Assessing, Monitoring, and Mitigating Aging Effects on Class 1E Equipment Used in Nuclear Power Generating Stations	X	
INL - Idaho National Laboratory		
INL/EXT-14-33129 - Advanced Instrumentation, Information, and Control Systems Technologies: Digital Technology Business Case Methodology Guide (2014)		X
NRC – Nuclear Regulatory Commission		
Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (2016)		X
NEI - Nuclear Energy Institute		
Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (DRAFT - 2016)		X

References

[B-1] IAEA SSR-2/1, Safety of Nuclear Power Plants: Design, International Atomic Energy Agency (2016)

[B-2] IAEA SSR-2/2, *Safety of Nuclear Power Plants: Commissioning and Operation*, International Atomic Energy Agency (2011)

[B-3] IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, International Atomic Energy Agency (2016)

[B-4] IAEA NS-G-2.3, *Modifications to Nuclear Power Plants*, International Atomic Energy Agency (2001)

[B-5] IAEA SSG-48, *Ageing Management and Programme for Long Term Operation for Nuclear Power Plants*, International Atomic Energy Agency (2018)

[B-6] IAEA NP-T-1.4, *Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants*, International Atomic Energy Agency (2009)

[B-7] IAEA TECDOC-1500, *Guidelines for Upgrade and Modernization of Nuclear Power Plant Training Simulators*, International Atomic Energy Agency (2006)

[B-8] IAEA TECDOC-1389, *Managing Modernization of Nuclear Power Plants Instrumentation and Control Systems*, International Atomic Energy Agency (2004)

[B-9] IAEA TECDOC-1402, *Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance*, International Atomic Energy Agency (2004)

[B-10] IAEA TECDOC-1066, *Specification of Requirements for Upgrades Using Digital Instrument and Control Systems*, International Atomic Energy Agency (1999)

[B-11] IAEA TECDOC-1016, *Modernization of Instrumentation and Control in Nuclear Power Plants*, International Atomic Energy Agency (1998)

[B-12] IAEA NSS33-T, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*, International Atomic Energy Agency (2018)

[B-13] IEC 61513, *Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems*, International Electrotechnical Commission (2011)

[B-14] IEC 60880, *Software Aspects for Computer-Based Systems Performing Category A Functions* International Electrotechnical Commission (2006)

[B-15] IEC 60709, *Nuclear Power Plants - Instrumentation, Control and Electrical Power Systems Important to Safety - Separation*, International Electrotechnical Commission (2018)

[B-16] IEC 60964, *Nuclear Power Plants - Control Rooms - Design*, International Electrotechnical Commission (2018)

[B-17] IEC 62645, *Nuclear Power Plants - Instrumentation, Control and Electrical Power Systems - Cybersecurity Requirements*, International Electrotechnical Commission (2019)

[B-18] IEC 62566, *Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*, International Electrotechnical Commission (2012)

[B-19] IEC TR 62096, Nuclear Power Plants - Instrumentation and Control Important to Safety - Guidance for the Decision on Modernization, International Electrotechnical Commission (2009)

[B-20] EPRI 3002002989, *Digital Instrumentation and Control Design Guide*, Electric Power Research Institute (2014)

[B-21] EPRI 3002002953, *Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments*, Electric Power Research Institute (2014)

[B-22] EPRI 1015087, *Instrumentation and Control Strategies for Plant-Wide and Fleet-Wide Cost Reduction*, Electric Power Research Institute (2007)

[B-23] EPRI 1002835, *Guideline for Performing Defence-in-Depth and Diversity Assessments for Digital Upgrades*, Electric Power Research Institute (2004)

[B-24] EPRI 3002004310, *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification*, Electric Power Research Institute (2015)

[B-25] EPRI 3002002852, *Advanced Nuclear Technology: Guidance and Methodologies for Managing Digital Instrumentation and Control Obsolescence*, Electric Power Research Institute (2014)

[B-26] EPRI 1020681, *Instrumentation and Control, Human System Interface, and Information Technology Requirements Project Plan for Nuclear Power Plant Long-Term Operation*, Electric Power Research Institute (2010)

[B-27] IEEE Std 1205-2014, *IEEE Guide for Assessing, Monitoring, and Mitigating Aging Effects on Electrical Equipment Used in Nuclear Power Generating Stations and Other Nuclear Facilities* IEEE (2015),

[B-28] INL/EXT-14-33129, *Advanced Instrumentation, Information, and Control Systems Technologies: Digital Technology Business Case Methodology Guide*, US Department of Energy Office of Nuclear Energy (2014)

[B-29] NRC SECY-16-0070, *Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure*, US Nuclear Regulatory Commission (2016)

Annex C | Simplicity in Safety I&C Design

Introduction

The 2018 IAEA Nuclear Energy Series report NP-T-2.11 [C-1] in section 3.6 addresses "elimination of unnecessary complexity in I&C" and refers to IAEA SSG-39 [C-2], stating that "unnecessary complexity should be avoided in the design of I&C safety systems". Especially for DiD Level 3 I&C systems (*e.g.* reactor protection system), the main focus should be on "simplicity in design" and avoiding complexity.

The discussion on "simplicity in safety I&C design" has several aspects and should be at least twofold. Therefore this annex differentiates between simplicity in safety ***I&C system design*** and in ***I&C component design***.
To identify the status on simplicity, it is essential to first provide the given definitions and criteria on simplicity and complexity respectively.

C-1 Defintions

Various (nuclear and non-nuclear) standards provide different definitions, so there is no broadly accepted definition.

The following definitions can be found:

Complexity:
1. Degree to which a system's design or code is difficult to understand because of numerous components or relationships among components.
2. Pertaining to any of a set of structure-based metrics that measure the attribute in (1).
3. Degree to which a system or component has a design or implementation that is difficult to understand and verify - ISO/IEC/IEEE 24765 [C-3].

Complexity matrix: A table used to allocate a weight to a function type.

Note: The matrix allocates this weight on the basis of the number of data element types in combination with the number of record types or file types referenced [C-3].

Complexity of a function: The weight allocated to a function on the basis of which a number of function points are assigned to the function [C-3].

Complex logic: An item of logic for which it is not practicable to ensure the correctness of all behaviors[1] through verification[2] alone - RIL-1101 [C-4].

Simplicity:
1. Degree to which a system or component has a design and implementation that is straightforward and easy to understand.
2. Software attributes that provide implementation of functions in the most understandable manner cf. complexity [C-3].

Simple hardware item: A hardware item is considered simple if a comprehensive combination of deterministic tests and analyses (summarized as "verification") can ensure correct functional performance under all

[1] This refers to behavior under all foreseeable operating conditions.

[2] Verification in this context means: Confirmation that specified requirements have been satisfied.
Note: In addition to verification, the demonstration of correctness of complex logic requires a combination of evidence from various phases of the development life cycle to be integrated with justification for completeness of coverage provided (summarized as development assurance).

	foreseeable operating conditions with no anomalous behaviour [C-4].
Dedicated functionality:	Property of devices that have been designed to accomplish only one clearly defined function or only a very narrow range of functions, such as, for example, capture and signal the value of a process parameter, or invert an alternating current power source to direct current. This function (or narrow range of functions) is inherent in the device, and not the product of programmability by the user IEC 62671 [C-5] [3,4].

C-2 Criteria

In many of these definitions, complexity contains several common components. In particular, complexity has been defined in terms of three separate dimensions within a particular system: **quantity, variety, and interconnections** [C-6][5].

Quantity refers to the number of items in a certain part of the system. The quantity could be, in the context of an I&C module, the number of components assembled to the I&C module, the quantity of input/output signals of a system, the number of buttons on a control panel, the number of I&C modules of an I&C system, or the number of subsystems within an overall system.

Variety is the number of different components in the system. Variety could refer to the number of different kinds of I&C modules applied within an I&C system or the different types of electrical or physical input signals.

Interconnections are the links between I&C components installed on an I&C module, the links between I&C modules of an I&C system or the links between I&C systems of the overall I&C architecture. These interconnections can be difficult to quantify in a given I&C module or I&C system, unless all states are known.

Complexity has been discussed by science for many years. Many methods such as "McCabe's cyclomatic" have been introduced to identify classification criteria, but such methods seem to be too "complex" for application to safety I&C.

C-3 Simplicity In Safety I&C System Design

Regulatory concerns generally treat this group as the most important:

- System interactions – algorithms that have feedback loops and extensive sets of inputs, since these aspects make it harder to assess all states for hazards.
- System interfaces – why are they needed? Are they well designed to be non-interfering? Is access controlled for any bidirectional connections? Interchannel communication is of more concern at the acquisition and processing layer than at the voting layer. Human-machine interface that can control safety equipment has also been a focus area.
- Operating systems – added complexity (*e.g.* interrupts, dynamic memory allocation, *etc.*) that make it harder to demonstrate deterministic performance.

[3] Ancillary functions (*e.g.* self-monitoring, self-calibration, data communication) may also be implemented within the device, but they do not change the fundamental narrow scope of applicability of the device.

[4] "Dedicated" in the sense it is used in this standard refers to design for one specific function that cannot be changed in the field.

[5] The given attributes are not necessarily negative but rather define the level of rigour in verification and validation.

There has been less concern with complexity for these aspects:

- Redundancies internal to a channel/train (*e.g.* TMR, 2-o-o-2 logic, redundant power converters, master/checker processor pairs) that are intended to improve reliability, increase fault tolerance, or minimize spurious actuation potential have been assessed but generally accepted without much concern.
- Self-testing that is internal to a platform chassis and intended to improve reliability and support graceful degradation has been assessed but generally accepted without much concern.

C-4 Simplicity In Safety I&C Component Design

Applying simplicity for I&C components of I&C Layer 0 (sensors & actuators) and I&C Layer 1 (field control devices) could avoid the need for unnecessary hardware (component) diversity.

Challenge 1: *Is it possible to identify I&C modules (e.g. for signal conditioning, priority management) or I&C systems as "Simple"/"Complex" (see Figure 1) based on figures on quantity, variety and interconnections in correlation with the demonstration measures?*

Figure 1. Simplicity vs Complexity

Challenge 2: *Which level/kind of diversity at the I&C module/I&C system level is required if sufficient evidence/analysis regarding simplicity could be provided (assessed by an "I&C system complexity analysis")?*

Note: This discussion becomes of high interest for defence-in-depth and diversity. Unnecessary requirements for diverse modules/systems increase the level of complexity and impacts overall safety of the plant. The request for diversity in each I&C layer/DiD Level should consider the level of complexity depending on the safety class of the I&C module/I&C system.

Challenge 3: *Complexity starts when causality breaks down.*

Causality is an abstraction that indicates how the world (a component) progresses. So a component could be identified as "simple" if all kinds of causes (input values + technological behaviour[6] and respectively all kind of effects (output values + technological behaviour) are 100% predictable,under consideration of postulated external influences.

Note: Radio Technical Commission for Aeronautics (RTCA) has published the document RTCA/DO-254 – Design Assurance Guidance for Airborne Electronic Hardware [C-7]. This focuses on guidance for simple electronic hardware, such as simple custom micro-coded components and devices, to assist applicants and developers in their demonstration of compliance, and to ensure their safe implementation in airborne systems.

[6] Covering: time behavior (ramp, pulse *etc.*), signal oscillation, expected min/max values *etc.*

Even if the document provides some figures on the assessment of simplicity, many applicants and developers are uncertain on several points such that the definition is ambiguous and may be interpreted differently. Currently still for aeronautics, there is no harmonized policy or guidance from the certification authorities to specifically address the safety and airworthiness requirements for simple electronic hardware.

References

[C-1] IAEA NP-T-2.11, *Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants*, International Atomic Energy Agency (2018)

[C-2] IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, International Atomic Energy Agency (2016)

[C-3] ISO/IEC/IEEE 24765, *Systems and Software Engineering - Vocabulary*, ISO/IEC/IEEE (2017)

[C-4] RIL-1101, *Research Information Letter 1101: Technical Basis to Review Hazard Analysis of Digital Safety Systems*, Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission (2015)

[C-5] IEC 62671, *Nuclear power plants – Instrumentation and Control Important to Safety – Selection and Use of Industrial Digital Devices of Limited Functionality*, International Electrotechnical Commission (2013)

[C-6] Sasangohar, F; Thornburg, K; Cummings, M L; D'Agostino, A*, Mapping Complexity Sources in Nuclear Power Plant Domains*, Human Factors and Ergonomics Society (2010)

[C-7] RTCA/DO-254 (EUROCAE ED-80), *Design Assurance Guidance for Airborne Electronic Hardware*, RTCA (2000)

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org

This report provides an overview of the current status and identifies the main difficulties the nuclear industry is facing regarding I&C modernization.

The Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group promotes the development of a worldwide regulatory environment where internationally standardized reactor designs can be widely deployed without major design changes due to national regulations.

I&C Modernization: Current Status and Difficulties