IAEA Nuclear Energy Series

No. NR-G-5.1

Digital Instrumentation and Control Systems for New and Existing Research Reactors

IAEA
International Atomic Energy Agency

IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A.3 and VIII.C of its Statute, the IAEA is authorized to "foster the exchange of scientific and technical information on the peaceful uses of atomic energy". The publications in the **IAEA Nuclear Energy Series** present good practices and advances in technology, as well as practical examples and experience in the areas of nuclear reactors, the nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues relevant to nuclear energy. The **IAEA Nuclear Energy Series** is structured into four levels:

(1) The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.
(2) **Nuclear Energy Series Objectives** publications describe what needs to be considered and the specific goals to be achieved in the subject areas at different stages of implementation.
(3) **Nuclear Energy Series Guides and Methodologies** provide high level guidance or methods on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.
(4) **Nuclear Energy Series Technical Reports** provide additional, more detailed information on activities relating to topics explored in the **IAEA Nuclear Energy Series**.

The IAEA Nuclear Energy Series publications are coded as follows: **NG** – nuclear energy general; **NR** – nuclear reactors (formerly **NP –** nuclear power); **NF** – nuclear fuel cycle; **NW** – radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA web site:

www.iaea.org/publications

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

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

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR NEW AND EXISTING RESEARCH REACTORS

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

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

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

IAEA NUCLEAR ENERGY SERIES No. NR-G-5.1

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR NEW AND EXISTING RESEARCH REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

COPYRIGHT NOTICE

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

Printed by the IAEA in Austria
April 2021
STI/PUB/1914

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Digital instrumentation and control systems for new and existing research reactors / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA nuclear energy series, ISSN 1995–7807 ; no. NR-G-5.1 | Includes bibliographical references.
Identifiers: IAEAL 21-01390 | ISBN 978–92–0–118320–0 (paperback : alk. paper) | ISBN 978–92–0–118420–7 (pdf) | ISBN 978–92–0–109621–0 (epub) | ISBN 978–92–0–109721–7 (mobipocket)
Subjects: Nuclear reactors — Control. | Nuclear engineering — Instruments. | Electronic instruments, Digital
Classification: UDC 621.039.5 | STI/PUB/1914

FOREWORD

The IAEA's statutory role is to "seek to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world". Among other functions, the IAEA is authorized to "foster the exchange of scientific and technical information on peaceful uses of atomic energy". One way this is achieved is through a range of technical publications including the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series comprises publications designed to further the use of nuclear technologies in support of sustainable development, to advance nuclear science and technology, catalyse innovation and build capacity to support the existing and expanded use of nuclear power and nuclear science applications. The publications include information covering all policy, technological and management aspects of the definition and implementation of activities involving the peaceful use of nuclear technology.

The IAEA safety standards establish fundamental principles, requirements and recommendations to ensure nuclear safety and serve as a global reference for protecting people and the environment from harmful effects of ionizing radiation.

When IAEA Nuclear Energy Series publications address safety, it is ensured that the IAEA safety standards are referred to as the current boundary conditions for the application of nuclear technology.

The IAEA's work in the area of research reactor operation and maintenance is aimed at enhancing the capabilities of Member States to utilize good engineering and management practices for the improvement of research reactor reliability and availability. In particular, the IAEA supports activities in addressing the ageing management of research reactor instrumentation and control (I&C) systems.

The purpose of this publication is to provide engineering guidance on the design, and operational aspects of digital I&C systems for the refurbishment of existing facilities and for new research reactors. This guidance is foreseen for the broad spectrum of research reactor types existing today. This publication is accompanied by on-line supplementary files that can be found on the publication's individual web page at www.iaea.org/publications.

The IAEA wishes to thank all those who contributed to this publication, in particular D. Jinchuk (Argentina). The IAEA officers responsible for this publication were C.R. Morris, R. Sharma and Y.G. Cho of the Division of Nuclear Fuel Cycle and Waste Technology and D.V. Rao of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

This publication has been edited by the editorial staff of the IAEA to the extent considered necessary for the reader's assistance. It does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

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

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

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

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

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

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Over half of the operating research reactors in the world are over 45 years old. During this time frame there have been significant advances in electronics, computers and networks, and these new technologies have been incorporated into the currently available digital instrumentation and control (I&C) hardware and software, for safety and non-safety research reactor systems.

Even though advanced digital I&C systems have been used extensively in many other industries, their use in the nuclear industry has been limited. This is mainly because the licensing process of digital I&C systems is complex and can be expensive. Despite these issues, numerous modernization projects have demonstrated that the functional improvements of digital I&C technology can provide cost effective improvements to the safety and operational availability of research reactors.

Instrumentation and control upgrades at operating facilities require the use of digital I&C equipment. While a digital I&C upgrade may be need based, it could be an effective means to enhance the facility's I&C system functionality, manage obsolescence, and mitigate the increasing failure liability of ageing analog systems. Many of the planning and implementation tasks of a digital I&C upgrade project are also relevant to the design and construction of new facilities since most equipment in new research reactors is likely to be digital.

The IAEA supports activities that address the ageing management of research reactor I&C systems, as well as the change from analog to digital technology. The aim is to enhance the capabilities of Member States to utilize good engineering and management practices for the improvement of research reactor reliability and availability.

This report is based on information from a consultants meeting held in 2011 and three IAEA technical meetings held in 2012, 2017 and 2019. In these meetings, a general publication outline was developed and then expanded to cover a range of programmes and activities considered to be significant. It reflects the experience from several projects carried out in different countries.

1.2. OBJECTIVE

The intent of this publication is to provide engineering guidance on the design and operational aspects of digital I&C systems for the refurbishment of existing facilities and for new research reactors. This guidance is for a broad

range of research reactor types, from low power research reactors such as the mini neutron source reactor to high power reactors such as the material test reactor. Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

1.3. SCOPE

Key areas addressed include code and standard applicability, licensing issues, dealing with the change in the human–system interface (HSI) from analog to digital technology, software verification and validation (V&V) activities, periodic testing and inspection, and configuration management. This report contains technical descriptions and summaries of available digital systems that have been utilized in both new research reactor designs and the upgrading of older analog safety and control systems.

This publication deals with two interconnected processes in the implementation of digital I&C systems: the construction phases and the licensing process. It provides guidance to owner/operators on several key issues for the modernization of I&C systems to ensure a smooth interface between the two processes.

It also gives guidance to research reactor operators intending to upgrade existing facilities from analog to digital systems or from older digital to newer digital technology and to governments or agencies seeking to construct a new research reactor facility utilizing the latest digital I&C systems. It is also of use to designers, vendors and regulators.

Even though this publication is technical in nature, it is intended mainly for those who will be involved in managing digital I&C modernization projects. It is not mandatory nor is it intended as a set of binding requirements that override national licensing requirements or internal owner and vendor practices. Rather, it provides information based on the experience of research reactor stakeholders. Each Member State has to develop its own project plan in conjunction with its regulations.

1.4. STRUCTURE

This publication is divided in two parts: a printed publication containing five sections and one appendix and supplementary files that can be found on the publication's individual web page at www.iaea.org/publications.

Section 1 of the print version is introductory. Section 2 presents general issues to be considered before embarking in an I&C project for a RR. Section 3 presents a summary of basic design principles and approaches to be used in the design of I&C systems, ways for demonstrating safety and early activities required in the planning of modernization projects. A description of the project phases is included in Section 4, beginning with the feasibility phase and ending with the handover phase. It also includes a description of the licensing process which is integral to the project. Section 5 includes the requirements and considerations for a completely new installation, which are in addition to those of a modernization project, where the process facility is newly designed and the facility is under construction. The Appendix provides a brief overview of related documentation from national and international organizations.

The second part of this publication, supplementary files, contains selected contributions made by Member States at various technical meetings regarding their experiences in performing upgrades or in the supply of new facilities digital systems.

2. GENERAL CONSIDERATIONS

2.1. RATIONALE

Research reactors rely extensively on I&C systems for providing functions such as protection, control, supervision and monitoring. I&C systems are vital parts of normal, abnormal, and emergency operations. As such, they have an important role in ensuring the safety of research reactors. Although analog I&C and measurement systems have operated satisfactorily in the past, research reactors are facing challenges in this area in terms of ageing and obsolescence of components and equipment. With continued licence renewals, the long term operation and maintenance of obsolete I&C systems may not be a cost effective and reliable option. The effort needed to maintain or increase the reliability and useful life of analog I&C systems may be greater in the long run than that of modernizing these systems or replacing them completely with new digital or hybrid systems.

There are several reasons for considering the modernization of some or all of these I&C systems in a research reactor. Obsolescence is a major consideration. This can result from causes such as lack of spare parts, supplier support and functional capabilities needed to satisfy current and future needs. Ageing of the I&C systems is another issue which leads to difficulties such as reduced

reliability and availability, increasing costs to maintain acceptable performance, and the lack of experienced staff for maintenance and engineering. In addition, the need for greater reliability and availability may require the capabilities of new technology that are not possible or practical with the older technology.

Refurbishments and licence extensions mean that a facility has to be supported longer, which will increase obsolescence issues. In addition, the older technology limits the possibilities for adding new capabilities to the facility systems and interfaces. New technology provides the opportunity to improve facility performance, human system interface functionality, and reliability; enhance operator performance and reliability; and address difficulties in finding young professionals with education and experience with older analog technology. In addition, there may be changes in regulatory requirements that could necessitate modernization activities.

2.2. ANALOG VERSUS DIGITAL TECHNOLOGIES

The most important difference between analog and digital technologies is that the latter rely on computers or other programmable devices. Hence, the software needs to be modified. The difference in capability between these two technologies is significant. Digital technology provides the ability to customize a generic system to specific facility functions, to use software to control facility equipment and to provide a large amount of information to operators in a small physical space. In changing the control system of a research reactor facility from an analog based system to a digital system, the following benefits have to be considered when analysing a modernization project:

— *Measurement precision:* Digital instrumentation, such as smart transmitters, are not likely to have the drift problems associated with the corresponding analog instruments. It is also possible to use digital technology to measure parameters more accurately than was possible with analogue technology.
— *Complex function capability:* Digital technology can easily implement complex functions since the software does not have the same limitations as hardware. Software is more versatile and usually does not require the addition of more and more components to change or add functions.
— *Adaptability and ease of modification:* Digital technology can be easily modified and expanded to incorporate new capabilities into the system since the implementation is in the software and not in the hardware.
— *Reduction in equipment volume:* Digital technology has the ability to process a large amount of data in one processor, reducing the size of the entire system.

— *Simplification of cabling:* Digital equipment has the great advantage of reducing cabling once all the necessary inputs are incorporated into the system. Cabling options such as multiplexing, and fibre optics are available for use in digital systems.
— *Reliability:* Digital technology can be used to achieve system reliability, for example by including a redundant processor that is in a standby state. In the case of a failure in the active system, the function of the system can be switched to the redundant standby processor with no interruption of system function.
— *Simplification of fault detection:* Digital technology can incorporate self-testing and self-diagnosis for fault detection.
— *Operator support:* Digital technology allows a large amount of data to be presented to the operator in a relatively small space using graphical computer screens rather than traditional hardwired indication panels. Alarms can also be devised in a way that assists the operator to diagnose a problem quickly.
— *Ease of system upgrading:* The system architecture of digital technology easily accommodates future version updates.
— *State of the art technology*: Digital technology is the current technology of interest for young engineers because of their familiarity with standard computerized equipment and because it is an integral part of their education. It is difficult to employ new engineers to work in nuclear facilities that utilize analog technology as they lack understanding of, and usually have little interest in learning, the principles of analog electronics. The recruitment of analog electronics engineers is becoming increasingly difficult, with most engineering experience and training in the digital systems and automation areas.
— *Maintenance costs:* Routine maintenance costs for digital systems are likely to be cheaper than the costs for analog systems (particularly with the price of digital technology dropping and the availability of helpful features such as built-in self-testing and self-diagnostics). However, major upgrades will be required due to lack of vendor software support or the unavailability of spare parts which may counteract these savings.

2.3. CHALLENGES

Digital technology, which incorporates software based control logic, provides a flexible, scalable solution to a facility's control needs. Due to the introduction of programmable components into an otherwise static analog system,

a number of challenges need to be considered while planning and executing a modernization project:

— *High development costs:* The development costs of new systems may be high due to the V&V and licensing processes of expensive, software based safety systems. The use of commercial off the shelf (COTS) equipment may reduce the development costs for software based safety systems because only custom configured items would require V&V to be undertaken, rather than the operating systems and platforms on which they are installed. The challenges of implementing a COTS based safety system is that the facility owner is dependent on the vendor for continued support in order to maintain the required qualifications of these systems in future upgrades. Also, the facility owner will be dependent on the vendor for repairs of failed equipment, including for even the most minor failures, in order not to void the formal qualifications of the system. These issues tend not to be relevant for non-safety systems where formal qualification is not required.
— *Software common mode failure risk*: Without suitable hardware and software architectures and proper development processes in the development of the new systems, there is a risk of introducing common mode failures through the software. This risk can be reduced through the proper use of V&V and diversity.
— *Quantified assessment of reliability:* If a quantified assessment of the reliability is required, for example, for probabilistic safety assessment purposes, it might be very difficult to come up with defendable reliability estimates for software based systems.
— *Retraining of operating and maintenance staff:* New systems may introduce the need for new training and skills in both the operations and the maintenance staff. On the other hand, these skills may be easier to find on the open market than skills in old analog systems.
— *Available standards:* There is an emerging body of standards available for digital systems, but it may be difficult to match the old standards with the new ones. There also seems to be less international consensus among licensing bodies on how to treat digital systems.
— *Acceptance by regulatory bodies:* Experience has shown that some national safety regulators are sometimes reluctant to accept computerized I&C systems.
— *Verification and validation:* Experience has shown that digital systems need a considerable amount of effort to ensure that they are functioning properly and that they are not exhibiting unintentional functionality in all operational modes.

— *Difficulty of identifying all possible defects:* Due to the complexity of digital software systems, it is difficult and requires specialized expertise and test tools to provide proof of completeness in all operational modes.
— *Short technological lifetimes:* Digital systems often exhibit rather short technological lifetimes. Therefore, it may be necessary to more proactively manage obsolescence as compared with the old analog systems. Key spares and shelf life issues need to be determined. The life cycle of digital system components needs to be addressed in the organization's maintenance and financial plans as they can be expensive when upgrading to a new architecture or technology. This cost might be justified by the extensive improved functionality and capability of the digital system.
— *Qualification of tools:* There are many computer based tools available for the design and V&V of digital systems. These may come from diverse industries such as the aircraft and military. The benefit of these tools may, however, be reduced due to the difficulty of proving they are producing the correct results.
— *Problems with staff acceptance and retraining:* The change of technology from analog to digital can sometimes be very extensive, and therefore may be difficult to get staff acceptance of the new systems. Early involvement of the staff when considering new, or different digital technology usually helps in this regard.
— *Computer security protections:* Ensuring computer security of the system protects the system's confidentiality, availability and integrity. National standards may need to be met as part of the licensing requirements. The demand for remote access to I&C systems and their associated data increases the risk of compromise by introducing new attack pathways. COTS digital systems have to be acquired from vendors having robust computer security programmes with demonstrated response to, and correction of, computer security vulnerabilities.
— *Security assessments:* With the migration to digital technologies and systems, additional attack paths could be introduced. An assessment approach should be used to verify the digital assets (DAs) and if they provide support and/or protection of critical functions. Based on the assessment, DA could be identified as a sensitive digital asset (SDA), which will require additional security controls to protect the functions and environments it supports. Computer security for research reactors is an ongoing subject, and Ref. [1] and other publications provide further information (see the Appendix).

2.4. MODERNIZATION AND NEW INSTALLATION PROJECTS

The complexity of digital I&C systems requires a comprehensive implementation plan to ensure that facility safety is maintained. This implies, for example, that all phases of design must include extensive V&V to ensure that due consideration has been given to systems functions and interactions between subsystems. An additional issue is that due to the incorporation of new computer and electronic components into digital I&C systems and the rapid, continuous rate of technology advancement, a well defined plan for obsolescence management is necessary.

Digital I&C systems have become the readily available technology for implementing various functions such as protection, control, supervision and monitoring functions at research reactors. When used correctly, digital technologies can provide far more functionality than their analog counterparts. However, it is important to be aware of the differences between the two technologies, especially during modernization projects. In most modernization projects, it is not feasible to replace all I&C system components in the facility simultaneously; therefore, special attention has to be given to the interaction between the existing systems and the new technology. In many cases, modernization requires more than just replacing existing systems by their digital equivalents, as the two systems are not necessarily functionally identical. Past experience from various projects in different countries has indicated that inadequate handling of the unique characteristics of digital I&C technology may unnecessarily delay the progress and increase the costs of modernization projects.

While many issues presented here are applicable to new facilities, in the case of a modernization project one has to consider some additional issues:

— It may be necessary to reconstruct the design basis of the facility;
— It may be necessary to update the design drawings as configuration management may be an issue;
— Even with an existing design basis, it may be necessary to interpret the facilities requirements for digital I&C;
— Adjustments may have to be made because the project has to adapt to the existing facility and its operational requirements.

During modernization, new software is introduced, which results in a new set of potential failure modes that have to be identified. The dominant failure mode of software based systems is deterministic in nature, which means that the use of redundancy alone does not necessarily provide a similar level of protection as in the original analog systems. In practice, this means that the implementation and licensing processes have to address such issues as protection against

common cause failures (CCFs) more rigorously than was necessary with analog based systems.

In addition to the introduction of software based protection and control systems as an issue for consideration, most industrial digital systems utilize standard, networking and computer operating systems that are well known and may contain vulnerabilities. The I&C modernization project must consider the information security requirements that are relevant to the operating organization and implement technological and administrative controls to protect systems from malicious intrusion. Specifically, the effects of compromise on system function which can lead to indeterminate design states or unexpected behaviour or actions (Ref. [1], paras 2.21–2.23) need to be considered. Failures, or no effect, are best case scenarios with respect to malicious compromise.

To manage a successful I&C modernization project, it is necessary to understand the roles and responsibilities of three major parties: the owner, the vendor and the regulator. The initiative to start a project comes from the owner, who has to investigate the possibilities to either acquire new, or modernize existing, I&C systems at their facility. Typically, this interest leads to the involvement of one or more vendors who can offer suitable products and may have previous experience from similar projects.

Once the initiation of an I&C project is considered feasible, the regulators are contacted to inform them about this intention and to discuss details of the required licensing process. If safety, or safety related functions are affected, the regulator will be involved in the process. After the feasibility studies are conducted, commercial negotiations are carried out and the project enters the implementation phase. In this phase, there is a need for interactions between all three parties (operator, vendor, and regulator), although formal communication always goes through the owner. This means that the owner is responsible for integrating all licensing requirements into the requirement specification documents that are presented to the vendor.

The owner is also responsible for documents that support the licensing process and may choose to include them in the contract between the organization and the vendor or prepare them internally. A project plan must be developed to ensure that all parties are aware of the time required for licensing approval, pre-installation testing, installation and commissioning. Possible hold points, for which regulatory approval is required before the project can proceed, must be included in the project plan and be stated in the contract.

To achieve this, all three parties have to coordinate their efforts. Large I&C projects could involve substantial costs, not only due to the equipment and services purchased, but also due to a loss of production, and the use of internal resources. It is therefore important for the three parties to assess the project risks early and assign suitable mitigation actions so that these risks can be reduced.

These mitigation requirements may have implications for the project plan, timeline and critical path. A further complication in large I&C projects is that all parties may involve their own subcontractors. It is therefore of utmost importance that individual responsibilities are clearly understood and documented.

Given the great differences in research reactor designs, there is a large range of possibilities for I&C modernization projects. Some projects may be of short duration while others may stretch over several years. In addition, the project may be undertaken primarily by the owner, may be a turnkey project supplied by vendors, or a combination of a system vendor contract and owner controlled contracts. Miniature neutron source reactors have upgraded to digital systems with relative ease whereas larger facilities have cancelled upgrades due to difficulties in licensing.

Due to this broad range of potential projects, this publication offers generic advice which is applicable to the majority of modernization projects and new facilities. Specific issues are identified and described for the project planning, execution, and licensing stages.

3. IMPORTANT CONSIDERATIONS FOR I&C SYSTEM MODERNIZATION

3.1. GRADED APPROACH

Research reactors are used in a wide range of activities such as core physics experiments, training, target material irradiation for materials science, transmutation doping, commercial production of radioisotopes, neutron activation analysis, experiments involving high pressure and temperature loops for fuel and materials testing, cold and hot neutron sources, neutron scattering research, and neutron and gamma radiography.

These uses call for a variety of different design features and operational regimes. As a result, site evaluation as well as design and operating characteristics vary significantly. Because of the wide range of applications, safety requirements may not be applied to every research reactor in the same way. For example, the way in which requirements are demonstrated to be met for a multipurpose, high power level research reactor might be very different from the way in which the requirements are demonstrated to be met for a reactor with very low power and very low associated radiological hazard to facility staff, the public and the environment.

The codes and standards used in the design of structures, systems and components (SSCs) have to be appropriately selected using a graded approach that takes into consideration the safety classification of SSCs, the potential radiological hazard associated with the research reactor [2] and the computer security of I&C system requirements based on a risk informed graded approach [1]. It is necessary to take a graded approach to the design of the I&C systems and keep it as simple as possible, not only for safety and security reasons but also for operational issues. Compared with nuclear power plants, research reactors generally have fewer personnel, lower budgets, and unique facility requirements and systems.

The graded approach may simplify regulatory approvals, thus reducing time and the budget. However, this approach always has to be justified, making some requirements less stringent with respect to nuclear power plant requirements. The justification has to demonstrate that safety and security are not compromised.

3.2. APPROACHES TO MODERNIZATION

Facility owners need to consider which approach is best for their facility before they embark on any modernization/refurbishment work. There are two possible, distinctly different, approaches to refurbishment:

(1) Multistep;
(2) All at once.

When using the multistep approach, it is important to conduct an impact analysis of the change in order to make sure that there are no resulting unintended consequences. Qualification of the entire system for the different steps of refurbishment may be required to ensure that the system still functions as originally intended. In either case, it is imperative to work within the scope of the operating licence and seek regulatory approval before the project is commenced. Each approach has different advantages and disadvantages, which are summarized in Table 1.

3.3. DESIGN BASIS DOCUMENTATION FOR MODERNIZATION

Once the intended scope of the modernization is defined, it is necessary to assess if the existing design basis documentation fulfils the necessary conditions as required by the I&C modernization project. It may also be necessary to reconstitute the design basis. This applies not only to the design basis of the

TABLE 1. APPROACHES TO MODERNIZATION

Approach	Definition	Advantages	Disadvantages
Multistep	Individual functions, parts or components are replaced one at a time	Likely the path of least licensing effort Potentially the lowest cost approach Allows time between changes to assess the new equipment Can be done during routine shutdowns and not impact normal facility operation schedules Computer security competence can be gradually matured focusing on limited digital technologies	Can take a significant amount of time Requires an impact analysis of the new component on the entire system May introduce unnecessary functionality if exact duplicates are not used May require a number of temporary interfaces to connenct the already modernized parts with the remaining old parts that will be modernized later Replacement of systems important to safety may require the requalification of the entire system Old and new systems may not be completely compatible
All at once	Major systems are replaced together (all field instruments, control systems, safety systems)	Improved compatibility amongst systems Generally provides enhanced system reliability The next generation replacement will be deferred into the future	Likely to be the path of most licensing effort particularly if an unknown supplier or unproven technology is selected Most complicated and expensive approach Loss of facility availability outside the routine shutdown periods may be required

TABLE 1. APPROACHES TO MODERNIZATION (cont.)

Approach	Definition	Advantages	Disadvantages
All at once	Major systems are replaced together (all field instruments, control systems, safety systems)	The cost difference between upgrading with the current system vendor and selecting a new vendor may be minimal	Generally has the higher risk ratings as there may be limited opportunity for reverting back to the original system in case problems arise Requires large scale up and maturity for computer security expertise to minimize introduction of vulnerabilities and management of risk

I&C systems or equipment, but also to the process systems to be controlled and monitored. The assessment of the design basis and its potential reconstitution may require considerable resources with the appropriate level of knowledge. In addition, it is necessary to comply with the requirements and boundaries of the safety analysis report (SAR) and the facility's operational limits and conditions. This is the underlying limiting condition for the requirement specification.

3.4. BASIC DESIGN PRINCIPLES

3.4.1. Codes and standards

The safety codes and standards used for research I&C modernization are contained in international standards such as the IAEA Safety Standards Series, International Electrotechnical Commission (IEC) Standards from Subcommittee 45A, Institute of Electrical and Electronic Engineers (IEEE) Standards and other national standards such as the GOST standards of the Russian Federation and the Commonwealth of Independent States. These system standards need to be used in conjunction with applicable standards for software and hardware. A list of some standards and related publications is included in the Appendix.

3.4.2. Safety demonstration

A safety demonstration, or safety case, is a demonstration performed by the facility for the regulatory body, to show that all phases of the development have

been performed such that the system meets the required safety level during the whole life cycle. The safety demonstration for an I&C modernization project, in one or several steps, must encompass the entire project life cycle, starting with defining the total scope of supply through commissioning, operating, maintaining, and modifying the new facility I&C system after integration in the facility.

The demonstration involves preparation of documentation and the collection and integration of evidence from verification, validation, and audit activities for all phases of the system life cycle. It has to include, but does not have to be limited to, the following parts:

— Modernization scope;
— Basic design principles to be employed;
— System requirement specifications;
— Functional specifications;
— Hardware and software designs;
— V&V process;
— QA and quality control.

For the safety demonstration, it is necessary to have procedures that enable changes to the design in a controlled and traceable way. The procedures must also cover how far back in the qualification process it is necessary to go to make sure that the change has not affected other parts of the qualification. An example would be if late in the development stage it is found that a qualified COTS product is not suitable for the application and a change of the selected product is necessary. This does not mean that the qualification process must start from the beginning, but it has to be brought back far enough to ensure that all traces of the disqualified product are removed.

3.4.3. Human factors assessment for human–system interface

It is necessary to prove, during the design process and its validation in the safety documentation, that all requirements for human–system interface (HSI) are met and that they comply with the criteria for safe and reliable operation of a research reactor facility. Verification and validation of the HSI design in relation to the functional and task analysis must include an analysis of the requirements applied by the licensing authority.

3.4.4. Classification and categorization

The terms ‘categorization’ and ‘classification’ are sometimes used as synonyms. For clarity in this publication, ‘categorization’ is reserved for functions and ‘classification’ for reactors and systems.

The importance of classification while planning an I&C modernization project is to ensure that sufficient attention and resources are allocated for the given system’s design, implementation, and V&V. The process to follow in a project is illustrated in Fig. 1.

Once the postulated initiating events (PIEs) and the safety objectives have been defined, the safety analysis of the facility can be developed. The first step is the categorization of the hazard that a facility poses to workers, the public and the environment. While the initial hazard categorization of research reactor facilities

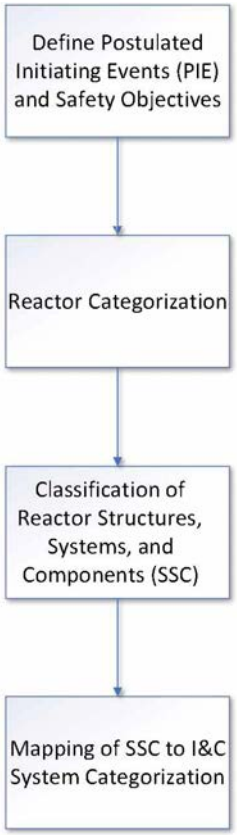


FIG. 1. Classification steps.

is primarily a function of power rating and radioactive inventory, it can also be affected by site characteristics [3].

Section 3 of IAEA Safety Standards Series No. SSG-24, Safety in the Utilization and Modification of Research Reactors [4], can be used as guidance for the categorization process. The consequences of sabotage of functions performed by I&C systems could also be associated with security levels. Such an approach would involve the State defining the threshold for unacceptable radiological consequences. The definition of a threshold for unacceptable radiological consequences may be based on quantitative or qualitative criteria, which can be expressed in terms of releases of radionuclides, doses or facility conditions [1].

3.4.5. Classification of structures, systems and components

The classification process places I&C systems and equipment into classes according to their importance to safety. These classes are characterized by sets of requirements on the properties of the system and its qualification. Fulfilment of these requirements determines the class. The requirements address the application functions, the service functions, and the system software functions, as appropriate.

All SSCs (including software for I&C) that are important to safety are required first to be identified and then to be classified according to their function and safety significance [5]. The requirements for design stipulate that the method for classifying the safety significance of an SSC be based primarily on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, and that account be taken of factors such as:

— The safety functions to be performed by the I&C system;
— The consequences of the I&C system's failure;
— The probability that the I&C system will be called upon to perform a safety function;
— The potential of the I&C system itself to cause a PIE and the combination of the probability and consequences of such a PIE;
— The timeliness and reliability with which alternative actions can be taken;
— The timeliness and reliability with which any failure in the I&C system can be detected and rectified.

Section 2 of IAEA Safety Standards Series No. SSG 37, Instrumentation and Control Systems and Software Important to Safety for Research Reactors [6], can be used as guidance for the classification of I&C systems.

3.4.6. Categorization of I&C systems

The categorization process places each I&C function into a category according to its importance to safety [4]. These categories are characterized by sets of requirements on the specification, design, implementation, verification, and validation of the I&C function, as well as by requirements on the minimal required class for the associated systems and equipment necessary for the implementation of the functions.

In all safety classification regimes used, there are technical and design requirements tied to each safety class. The requirements are more relaxed in the lower categories. Following this principle, the SSC, including software for digital I&C systems, are designed such that their quality and reliability are commensurate with the safety class they belong to. The highest requirements are imposed on systems and functions belonging to the highest safety class. These systems and functions are usually restricted in their functionality, following basic design principles that systems and functions belonging to the highest safety class have to be as simple as possible and on which detailed analyses can be done. Another important design principle ensures that any failure in a system belonging to a lower class will not propagate to a system classified in a higher class. Following these design principles will facilitate the licensing process. It is also important that the technical and design principles tied to each safety class are agreed on between the licensee and the regulator before the design is started.

The method for classifying the safety significance of a function has to be based primarily on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, with account taken of factors such as:

— The safety function(s) to be performed;
— The role of the function in preventing or mitigating consequences of PIEs;
— The role of the function during all normal operating modes (startup, operation, shutdown), as well as during refuelling or accidents;
— The role of the function following PIEs such as natural events (seismic disturbance, flood, extreme wind, lightning) and internal hazards (fire, internal flood, missiles);
— Radioactive release from adjacent unit or chemical releases from other facilities or industries;
— The consequences of failure of the I&C functions;
— The effects of spurious actuation of the I&C functions;
— The probability that it will be required to perform a function important to safety;

— The time following a design extension condition (DEC) at which, or during which, it will be required to operate.

It will not be possible to identify in detail all the functions at an early stage in the design process, as the characteristics of the facility will not yet have been fully defined. The process of identification and classification of the functions therefore has to continue iteratively throughout the design phase. Where an initial assignment of a function to a class is uncertain, an explanatory note has to be added to the classification documentation.

The International Electrotechnical Commission (IEC) categorization defines three safety categories A, B and C, while the US Institute of Electrical and Electronics Engineers (IEEE) only distinguishes between safety and non-safety systems. The IAEA defines items important to safety and items not important to safety. Items important to safety include safety systems and safety related systems. IAEA Safety Standards Series No. SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants [7], provides guidance on the categorization of functions to the three categories and classifies respective systems accordingly.

3.4.7. Defence in depth

In general, it is the safety analysis of the facility that demonstrates the adequacy of dedicated systems implemented at different levels of defence in depth.[1] The concept of defence in depth is implemented with due account taken of the graded approach. For example, for 'low power' research reactors the postulation of accident conditions (i.e. design basis accidents and DECs) may not lead to unacceptable radioactive releases and therefore the fourth or fifth level of defence in depth may not be needed.

According to IAEA Safety Standards Series No. SSR-3 [5] and the International Nuclear Safety Advisory Group [8], the design of research reactors must consider five levels of defence in depth. Thus I&C systems have to integrate several levels of defence in depth, as shown in Fig. 2.

At a minimum, research reactor I&C systems have to incorporate the following levels of defence in depth:

— At the operational level for normal and anticipated operational occurrences;

[1] The concept 'defence in depth' is used here to refer to 'safety defence in depth' as described in Ref. [5]: "A series of levels of defence … that are aimed at preventing accidents and ensuring adequate protection of people and the environment against harmful effects of radiation …."

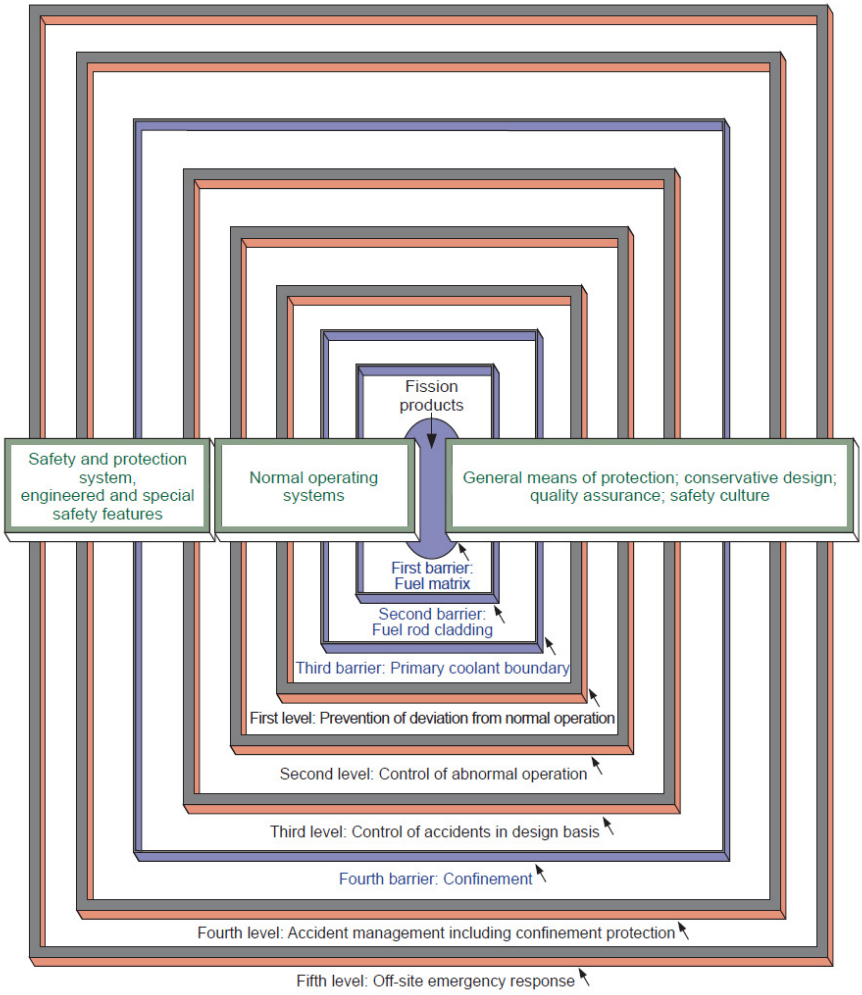


FIG. 2. The principle of defence in depth [9].

— At the safety level for design basis accidents if I&C systems are required to perform any mitigating actions;
— The fourth level of defence in depth, which is considered for DECs, deals especially with CCFs in digital reactor protection systems. This is achieved by dedicated equipment, or other equipment not used in the previous level of defence, to ensure independence between two successive levels of defence in depth.

IAEA Safety Standards No. SSR-3 [5] requires consideration of the following aspects:

— Use of conservative design margins and the implementation of a quality assurance programme for developing the entire I&C system (not the safety part only);
— Provision of successive actions to prevent, control or mitigate accident conditions;
— Application of the single failure criterion to each safety group performed by the reactor protection system.

Regarding defence in depth against security compromise,

> "it should be applied to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level. Defence in depth against compromise involves providing multiple defensive layers of computer security measures that must fail or be bypassed for a cyber attack to progress and affect an I&C system. Therefore, defence in depth is achieved not only by implementing multiple defensive layers (e.g. security zones within a defensive computer security architecture), but also by instituting and maintaining a robust programme of computer security measures that assess, prevent, detect, protect from, respond to, mitigate and recover from an attack on an I&C system" [1].

Technical guidance to protect against computer security vulnerabilities is provided in IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [10].

3.4.8. Reliability

As explained in Ref. [6], reliability is an important attribute of systems important to safety. These systems need to be designed such that their quality and reliability are commensurate with their safety classification. To ensure these design basis reliability requirements are met, a suitable combination of probabilistic and deterministic criteria must be applied.

With the importance of safety, an I&C system's reliability also must be higher. However, where practical limits of reliability of individual components are reached, the need to achieve higher levels of reliability is satisfied by using redundancy, independence and diversity. The use of redundancy provides protection against single failure criteria, while the use of diversity and independence provides protection against CCF.

3.4.9. Single failure criterion

According to Ref. [5], it is required that "the single failure criterion shall be applied to each safety group incorporated in the design of the research reactor". This means that each I&C safety system should be capable of performing its task in the presence of any single failure. A single failure is a one which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it. The single failure could occur prior to or at any time when the safety task is required, and it is mandatory that all identifiable failures in I&C safety systems be detectable by anomalous indication, alarm, or periodic testing.

3.4.10. Redundancy

For all I&C systems important to safety, the principle of redundancy must be applied to meet the design basis reliability and to prevent the safety consequences of single failures, as well as to improve availability and maintainability. The degree of redundancy has to reflect the level of reliability required for the safety system.

Multiple sets of equipment that cannot be tested individually cannot be considered as being redundant. For very high levels of reliability, the use of redundancy is limited by the CCF rate of redundant channels given that there is no diversity between these channels.

3.4.11. Independence

As mentioned in Ref. [5], the principle of independence (electrical and functional isolation or physical separation by means of distance and barriers) has to be applied to enhance the reliability of a system and its capability to resist to CCFs. According to Ref. [6]:

> "Independence is intended to prevent the propagation of failures from the item affected by the failure to other redundancies, or from one system to another system independent of the safety class to which they belong.
>
> "The instrumentation and control system architecture should not compromise the independence in effect at the different levels of defence in depth.
>
> "Safety systems should be independent of systems of lower safety classification to ensure that the safety systems can perform their safety functions during and following any postulated initiating event that requires

these functions without any interference or degradation from systems of lower safety classification.

"The failure of the support features of safety systems should not compromise the independence between redundant components of safety systems or between safety systems and systems of lower safety classification."

When isolation devices are used between safety and non-safety systems the isolation devices has to be considered part of the safety system.

3.4.12. Diversity

According to Ref. [11], diversity in I&C systems is the principle of monitoring different parameters, using different technologies or different algorithms, in order to provide several ways to respond to a significant event. Diversity is used to prevent CCFs:

"The use of diversity, redundancy and independence (i.e. physical separation, and electrical and functional isolation) in the architecture of the instrumentation and control systems should be consistent with the safety classification of each instrumentation and control system, and with the defence in depth concept, both for the overall facility and for the instrumentation and control system. In the case of redundancy, other factors such as reliability (i.e. the probability that a system or component will meet its minimum performance requirements when called upon to do so) or the availability of instrumentation and control systems should be considered." [6]

Different types of diversity may be considered, including human diversity, functional diversity, signal diversity, equipment and system diversity and software diversity. It is important to note that different manufacturers might use the same processor or licence for the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers' names are insufficient without consideration of this possibility.

The principle of diversity has to be adopted wherever practicable, after consideration of its possible disadvantages in terms of complications in operating, maintaining and testing the diverse equipment:

"The instrumentation and control system should have a fail-safe design such that no malfunction within the system caused solely by variations of external

conditions within the ranges detailed in the design basis would result in an unsafe condition or failure." [6]

3.5. DIGITAL TECHNOLOGY

For modernization projects where digital I&C is to be used, there are many different options available, from proprietary systems to custom built equipment: supervisory control and data acquisition systems and distributed control systems; microprocessor based and field programmable gate array based systems; and nuclear qualified and non-qualified equipment. The categorization process and the determination of the basic design principles to be satisfied will determine the best option for the facility.

3.5.1. Commercial off the shelf components and qualification process

In the nuclear industry the suppliers of nuclear qualified equipment are decreasing in number and there is thus a corresponding increase in the cost of such equipment. Therefore, it is advantageous to use the lower cost and extensive history of widely used non-nuclear qualified COTS equipment if it can be shown to meet the same quality requirements. As a result, it has become common for nuclear facilities to purchase non-nuclear qualified COTS equipment and qualify it for use in safety systems. This is done by developing a qualification process to ensure that a desired level of quality can be obtained from COTS equipment and for any customized components developed and produced for the facility.

For customized digital I&C equipment and software developed for nuclear applications, the required assurance is developed by controlling and monitoring the software design and development process, as well as through formal V&V programmes.

In general, non-qualified COTS equipment can be used in research reactor facilities for non-safety applications if it meets the facility's performance standards. These standards are usually satisfied by choosing proven, high reliability systems that are widely used and have an acceptable performance record in other industries. However, in applications whose performance can affect the nuclear safety of the facility, and the facility licensing basis, a higher standard has to be met and the regulatory authorities has to be satisfied that the performance and quality of a given item are compatible with the conditions of the licence. For these applications, an agreed method is needed for assessing and qualifying the items for their intended service.

COTS equipment and software used in systems that are classified as safety category 1E, or A, have to be qualified and/or developed according to

the specific nuclear standards chosen by the facility operator. The use of COTS also necessitates the consideration of security requirements and a review of the services and capabilities provided by the COTS systems and components. A hardening guide should also be developed for the specific system to provide the implementation requirements to maintain a safety and security environment.

3.5.2. Common cause failure

Safety systems in research reactors have to reliably satisfy their functional requirements. In order to achieve this goal, safety systems are designed to be functional when a single failure is evident; that is, no single failure is to prevent safety system actuation if needed, nor must a single failure cause a spurious activation of the safety function. However, the system has to be designed to reveal these failures through alarm systems or during testing.

Failures of two or more SSCs, due to a single specific event or cause, are categorized as CCFs. In essence, a CCF can be defined as a failure that impacts multiple items or portions of a system and a failure that affects multiple redundancies of the same system. CCFs can occur due to common external or internal influences. External causes may involve operational, environmental, or human factors. The internal common cause could be a design error that creates a common dependency on supposedly independent redundancies, for example a shared power supply.

Examples of systematic failures usually include human errors in design, operation, and maintenance. Also, other external factors like heat and vibration can still be accounted for in systematic failures. Such failures may impact a redundant or non-redundant system. To protect against common design errors, the design could include a diversity of components that involves components with different internal designs but which perform the same function.

A second type of diversity is a functional diversity, which involves components that perform completely different functions at the component level. An example of functional diversity is the use of high reactor power flux to cause a reactor trip using control rods and high coolant temperature to cause a reactor trip using moderator removal. Diversity in this case involves using different principles of operation and reactor properties (neutron absorption and neutron moderation) to satisfy the same system level requirement to bring the reactor to the subcritical state.

3.5.3. Common mode software failure

Digital technology introduces the possibility that common mode software failure may cause redundant safety systems to fail in such a way that there is a

loss of safety function. This type of failure is important in both the installation of digital components in existing facilities and in new facility design. In older facilities, where digital components are being substituted for analog ones, assumptions about the independence of components may have been made in the original licensing basis. If these assumptions can be invalidated by the introduction of the digital components, then the safety evaluation has to be redone using the new assumptions. In new facilities, if the use of digital components can invalidate standard assumptions and procedures for achieving and assessing independence and high reliability, then new procedures may be needed.

The defence in depth and diversity of the new I&C systems must address their vulnerabilities to common mode failures, including the possibility of software design or operational errors. It is recommended to analyse each postulated common mode failure for each event that is considered in the SAR using best estimate methods.

If a postulated common mode failure has the capability to disable a safety function and the failure cannot be eliminated by design, then a different means must be used to perform either the same or alternative operation to ensure that the safety function is not compromised. The different operation may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. However, trying to licence this non-safety system to perform this function may be exceedingly difficult. It is strongly recommended in these instances to work very closely with the Member State's regulatory body to ensure it will be an acceptable alternative.

Diversity between automated digital and non-digital systems is considered to be acceptable. Manual actions from the control room can only be given credit in the safety analysis if time and information are available to the operators. The extent and types of diversity may vary among designs and must be evaluated individually according to the requirements of the facility.

3.5.4. Human–system interface

Digital I&C systems require careful consideration of human factors and human–system interface issues. The success in using new technologies is based on a designer's ability to reduce incompatibilities between the characteristics of the system and those of the people who operate, maintain, and troubleshoot it. It is important to have a well designed operator interface for reliable human performance and nuclear safety. Safety depends, in part, on the extent to which the design reduces the chances of human error and enhances the chances of error recovery (or safeguards against unrecovered human errors).

In both the modernization of existing research reactors and the new builds, the use of computer technology, computer based interfaces, and operator aids

raises important issues related to the way humans operate, troubleshoot, and maintain these systems. Two human–system interaction issues frequently arise with the introduction of computer based technology:

(1) The need to address a class of design errors that persistently occur in a wide range of safety critical applications or recur in successive designs for the same system, for example duplicating code for application in different process systems or transmitting the same error through various operator interfaces;
(2) Defining the role and activities of the human operator with the same level of rigour and specificity as system hardware and software.

Some deficiencies in the design of computer based technologies include data overload, misleading information, and lack of consistency. Data overload can be created by the presentation of an excessive amount of information on poorly designed computer screens or the design of an alarm system which does not mask alarms generated by normal facility conditions. The use of a clear colour palette and a library of standard symbols are important to create an interface which is intuitive to operators and is easily used to create a consistent human–system interface.

The human interaction in new computer systems must be carefully designed and evaluated in the context of nuclear applications. Navigation through the systems must be simple and developed in a hierarchical way so that operators can be trained to find information quickly. Ergonomic and anthropometric aspects of the human–system interaction must also be considered so that the interface can be used comfortably, reducing operator fatigue.

An effective methodology is essential for designers, owner–operators, maintainers, and regulators to assess the overall impact of computer based, human–system interfaces on human performance in nuclear research facilities. Reference [6] provides guidance on the human–machine interface and human factors engineering.

As an example of local standards used for this purpose in the United States of America, the standard from the United States Nuclear Regulatory Commission (NRC), NUREG-0700 [12], is used as guidance for incorporating advanced human–system interaction technologies in existing nuclear power plants, typically complemented with NUREG-0800 [13]. They propose both a methodology for reviewing the process of design of the human factors elements of control rooms and specific guidelines for evaluating a design product.

In new or refurbished facilities, NRC standard NUREG-0711 [14] can be used as a guideline for designing the human–system interface, taking into account the sections relevant to research reactors.

3.5.5. Security aspects

The use of digital computers and networks for I&C systems raises the issue of computer security in research reactor facilities. Security control for an unauthorized access to facility systems through the internet or other paths must be strengthened.

Computer security therefore has to be considered in a digital research reactor modernization project or new build and has to be systematically incorporated into an I&C system design from the conceptual stage. It is strongly recommended to develop a computer security programme, policies and detailed plans in accordance with any national requirements, the regulatory guides or industry IT best practices.

Computer security has become a very important topic with regulatory bodies due to potential attacks. It must be noted that the processes are similar to safety ones and the high level goals and objectives are the same. Details of how to incorporate computer security can be found in IAEA Nuclear Security Series No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [1], and other guides and publications, such as those listed in the Appendix.

3.5.6. Ageing management considerations

Due to the shorter life expectancy of digital technologies in comparison to analog, it is necessary to consider the issue of hardware and software obsolescence and how to manage it during the life of the facility. A plan for ageing management needs to be addressed during the design phase. Both refurbishment and new build projects often require significant time to complete; as a result, some components of the system may be approaching obsolescence and will need to be replaced a few years after completion.

To maintain the reliability, availability and maintainability of the digital systems, the owner will have two main options:

(a) Maintain communication with the different suppliers and implement a programme of upgrades when equipment and software reach the end of their normal life. This life is dictated by the supplier. For digital control systems this life could be anything from 3 to 20 years, depending on the equipment. For other digital I&C equipment the expected life expectancy is about 10 years, but could be from 7 to 15 years, depending on the technologies. It is important to plan for future upgrades resulting from operating system revisions and changes which can also determine the necessity to upgrade

hardware. This is normally expected every three to five years, which is commensurate with the time required to complete a modernization project.

(b) The owner manages the continued use of components and equipment to extend the life beyond the normal industrial time frames by:
   — Ensuring availability of the equipment's replacement parts (mainly components and cards), maintenance tools and documentation;
   — Ensuring that qualified technicians are always available and are continuously checking the availability of externally supplied components.

In practice, a mixed approach between these two options will occur, but it is recommended that facility operators:

— Are independent from their suppliers to build an independent risk assessment for the possibility of obsolescence of the different types of digital equipment during the operational life of the facility and to build the method to anticipate it;
— Consider, in the design phase, the availability of spare parts to preclude the requalification of the entire I&C system because of new components.

3.6. ARCHITECTURAL APPROACH

To design the architecture of an I&C system, it is necessary to consider the following aspects.

3.6.1. Functional aspects

I&C systems provide the solutions to implement the functional requirements generated by process designers. The high level description of the requirement specification (which is a description of the problem to be solved), independent of any specific technical solution (why a particular system is an appropriate solution to solve the problem), has to be explicitly identified as the main input data.

This requirement specification will permit the I&C system designer to:

— List the functions to implement in the I&C systems as well as the complexity of these functions, the associated performance (time response and accuracy) and the operational constraints (dependability requirements, environmental conditions and operational cycles);
— Define the scope of the processes to be controlled by a centralized I&C system, as opposed to those using decentralized or local ones;

— Estimate the level of scalability required in the I&C system to meet the specific requirements of the facility (be able to meet future requirements for expansion of the facility itself or for the permanent or temporary addition of experiments).

Note that for safety and economic reasons, a simpler and scalable solution is the advisable approach.

3.6.2. Safety aspects

The safety requirements placed on the I&C system have to be considered with the following two complementary considerations:

(a) The specific regulatory requirements and the normative prescriptions to be considered according to the safety standards applicable to the facility (e.g. choosing the IEEE approach with classes 1E and non-1E of I&C safety items versus the three IEC classes A, B, C). Included in this are the requirements of the applicable national or state safety authorities.
(b) The specific safety analysis of the facility has to be taken into consideration because of the wide range of research reactor designs and purposes with differing safety cases. The design of the I&C system has to consider:
    — The specific features of the facility;
    — The PIEs identified in the facility safety analysis and the associated I&C required to mitigate their consequences;
    — The levels of the defence in depth to be implemented.

Safety Reports Series No. 55, Safety Analysis for Research Reactors [15], states:

"When upgrading the instrumentation and control systems, improvements in the coverage of PIEs may lead to changes in the accident sequences and rules of analysis; for example, addition of a low core pressure drop trip variable as a redundant and independent means of detecting loss of core cooling flow will change the loss of flow accident (LOFA) sequence" (Section 5.2.2).

This aspect must be analysed for the modernization of I&C.

Regarding the principle of defence in depth, it is important to clearly explain how this principle has been implemented in the chosen architecture. It is also necessary to demonstrate a clear and strong separation between successive levels of defence in depth and also between safety and non-safety systems.

3.6.3. Technological aspects

The architecture of an I&C system has to be chosen with the appropriate technologies and products to meet the functional and safety requirements. There will ultimately be a compromise between the following:

— The cost to purchase the products, but also to qualify and maintain qualification of the safety systems during the life of the facility;
— The risks of the obsolescence of technologies/products and of the lifetime and availability of the providers themselves;
— The flexibility provided to operate the facility with the chosen products and architectures;
— The feature of customization of most of the research reactors and the available COTS solutions and a standard product;
— The ability to licence these solutions with advantages in purchasing pre-certified products and/or proven technologies;
— The difficulties for small I&C teams to maintain systems that are technologically complex;
— The additional initiating events to be taken into account in the safety analysis due to the technological choices.

3.6.4. Hybrid technical solution architecture as an alternative

As software based systems have greater risk due to the introduction of common mode software failures, the modernization of I&C systems can be based on the design of hybrid systems. The combination of digital technology with hard wired technology helps in obtaining a hybrid system that allows the execution of a function using both technologies simultaneously in a redundant and diverse manner.

The use of hard wired/digital modular protection systems — where the safety functions are carried out by hard wired electronics and the supervision function by the microcontrolled (digital) layer — facilitates self-diagnostic functions and communication through isolated unidirectional buses to the reactor control and monitoring system.

3.6.5. An iterative process of design

The compromise between the functional, safety and technological requirements must be determined using an iterative design approach involving these three considerations, as shown in Fig. 3, rather than in a sequential approach.

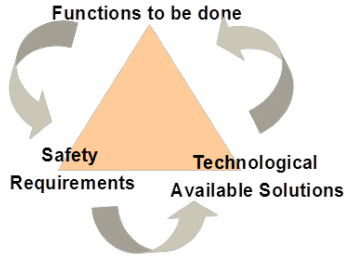


FIG. 3. Iterative process for requirements specification development.

It is necessary to identify, at the beginning of the design phase, the milestones for the preliminary and final overall I&C system architecture after some reasonable iterations of these three stages. This will ensure that all design teams are included in the considerations in a timely manner and that there are chances for the design to be improved.

3.7. CONSIDERATIONS DURING THE PREPARATION OF THE MODERNIZATION PROJECT

3.7.1. Planning

Any I&C project has to be placed within the general framework of plant life management. This means that the necessary relationships with other potential or planned modifications must be considered in the planning of the I&C project. The need for future modifications may emerge from a range of considerations, such as adaptations to new regulatory requirements or replacing obsolete facility equipment. Planning for future modifications is especially important for digital technology because the lifetime of digital systems is typically much shorter than that of the facility. This may create the need for more than one upgrade of the same system during the facility lifetime. Designing reusable requirement and functional specifications can, at least, partly address this need.

Although no specific guidelines can be given for the type, scope and sequence of an I&C modernization project — since each one depends on project constraints and factors which differ from facility to facility — some general guidelines can be found in Section 10 of IAEA Safety Standards Series No. SSG-37 [6].

In the planning of I&C projects, it is also wise to investigate the possibility of increasing the facility's safety and capabilities by introducing new functions in the I&C system. It is a good idea to involve two or more vendors during

the generation of a pre-project conceptual study to establish basic design philosophies. This arrangement also provides an opportunity for the facility to learn about the available technologies as well as opportunities for the potential vendors to acquire an understanding of the facility design and the intent of the modernization.

A project leader must be appointed early in the project. The leader must have a very broad and deep understanding of the operation of the research reactor and its I&C systems. This person will have to mediate between the involved parties and ensure that the project is successfully completed. There are many potential sources of resistance against a modernization project from many areas within the facility organization, even if the need is recognized and accepted. Thus, it is essential that the project leader is supported by management personnel at the appropriate level. The project leader will require a team of engineers to assist in the details of the project. These tasks include preparing the requirements specifications, tender evaluations, testing, installation and commissioning activities and possibly training.

3.7.2. Specific considerations

When modernizing I&C systems it is usual to consider the possibility of enhancing the safety of the facility during the modernization. Sometimes a limited redundancy in the actual process components, such as sensors, sets a limit on what can be achieved. It may be possible to build in additional safety functionality within the digital I&C system to compensate for a lower level of redundancy in the process components.

I&C modernization may introduce the need to undertake a complete revision of the protection philosophy, especially in the case where protective devices are introduced that cannot meet the failure probability requirements. When the safety requirements have changed, such as a greater reliance on the probability of failure on demand for a safety function, an application of the requirements in the design basis may introduce conflicts between different protective signals. In a simple case this may occur, for example, when smart devices introduce the possibility of component protection (e.g. of valves, pumps). If the major protection signal is not allowed to override the component protection, the functions may not be available on demand (undermining the reliability claim) due to a fault in the component protection (e.g. critical pump motor shut off protection as a result of component protection). The correct way to resolve such issues is to prioritize the safety functions of major components and the devices by which they are controlled. Claims on manual control may be another way to mitigate shortfalls in the automatic safety function by allowing the operators to manually

override the component protection, but the operator needs time and sufficient information to proceed.

Another possible conflict may emerge if a diverse protective system is required for a safety function in the highest safety category. The priority between the primary and the diverse systems and their conditions for an initiation must then be defined independently and precisely for each of their functions. For example, one of the systems may have been installed as part of a very simple and comprehensively tested platform and the other using a more sophisticated platform. The practical solution would be to use the more sophisticated system as the first barrier and to use the simpler system as the second line of defence to meet the requirements of the safety case.

Modern digital technology has a wide variety of beneficial capabilities compared with analog technology. Therefore, in many cases simply replicating the capabilities of the old system with new technology is not the best solution for the facility.

When a new system is being implemented, the potentially beneficial capabilities of the new technology must be evaluated to determine which are appropriate for inclusion into the system to achieve facility goals, such as increased reliability and availability. The following must be considered:

— For each change option proposed, the risks to the goals of the facility have to be identified and evaluated to include safety, environmental and business risks;
— Depending on the scope of the I&C modernization, some existing sensors may be replaced and other old ones may be reconnected to the new I&C system;
— In the case when the new I&C system utilizes existing sensors, special care must be exercised to ensure their compatibility with the new system. This means, for example, that accuracy requirements and time constants have to be defined for the interface equipment;
— It may also be necessary to ensure that the new equipment is qualified for the likely conditions to be experienced in the locations in which they are placed to ensure that they meet their safety requirements under all possible conditions.

3.7.3. Risk assessment

Risks must be identified by competent staff within the facility with the necessary level of management oversight, involvement and support. Changes which pose the most significant risk must be reviewed by independent persons, review groups or individuals at a proportionally higher level in the facility to

ensure that a comprehensive evaluation has been prepared. Research reactors must have an independent safety organization in place, in which case this would be the obvious choice to carry out safety and security reviews of the risks associated with the proposed changes. Regulators may review the evaluation of the risks for a proposed change and may impose regulatory holds on changes they feel are safety significant.

The risks must be identified and evaluated in terms of:

- Risks introduced to the facility for the proposed change for both project implementation and subsequent system operation;
- A risk matrix showing the relationship between likelihood, consequence and risk level;
- The likelihood of the risk occurring;
- The consequence of the risk on the facility or project;
- Acceptable or unacceptable risks;
- The mitigation strategies used to reduce the risk to an acceptable level;
- The costs of implementing particular controls relative to the benefits obtained in managing the risks.

Risk evaluation must use appropriate generic industry information relevant to the reactor type and operating experience. For some changes, it could be possible to use deterministic or PSA methodologies to make risk informed judgments. The risk evaluation must focus on the safety performance of the facility and the modernization project's success.

The documented risk evaluation must include:

(a) The reason for the change:
    - Inputs for the proposed change;
    - Interfaces;
    - Performance evaluation.

(b) Description of the outcomes of the change:
    - A high level description of the proposed change;
    - Detailed description of the improvements to the organization;
    - The tasks, responsibilities and stages of the proposed change.

(c) Evaluation of the proposed change, the implementation strategy and the expected benefits/outcomes, such as the impact on:
    - Safety;
    - Computer security;
    - Interface between safety and security;
    - Performance;
    - Responsibilities and accountabilities;

— Processes;
— Decision making;
— Internal interfaces;
— Priorities;
— External challenges;
— Financial performance;
— Cost bases;
— Competitiveness;
— Human resources:
— Optimization of staff numbers;
— Working locations and conditions;
— Personal accountability;
— Communications (participation in decision making at all levels);
— Personnel competencies.

All modernization steps have to be completed in such a way that the levels of facility safety and availability are ensured at any time. For project implementation being undertaken during the reactor's routine shutdowns the facility has to be able to be operated with the required levels of safety and availability over long, or even unlimited, time periods. This has to be taken into consideration in the risk assessment and in the implementation strategy, and may also dictate which vendor is chosen, or which technical solution is preferred.

4. I&C PROJECT EXECUTION

4.1. OVERVIEW OF PROJECT PHASES

The modernization project can be organized into various phases: the feasibility phase, the requirements specification phase, the preliminary and detailed design phases, the manufacturing and procurement testing phases, the installation and commissioning phases, and the handover phases. Licensing is an integral part of all of these phases and must be considered at every critical point in the project.

4.2. MODERNIZATION PROJECT PHASES

4.2.1. Feasibility phase

Regardless of the reason for modernization of an I&C system, and whatever is the intended strategy, some basic investigations have to be performed, starting with a pre-project plan that considers the facility's life cycle management plan and a feasibility study. The issues to be considered are the same for all types of modernization projects, regardless of whether they are done in one step or several steps.

One of the most important project constraints is the intended remaining operational lifetime of the facility. Large modernization projects may not be economically justifiable when the remaining operational life of the facility is short. The payback time on a medium to large scale modernization project may be needed to justify the estimated expenditure. As the remaining lifetime decreases, choosing the start time and establishing a schedule for the I&C modernization project becomes more important. A common goal is to avoid the need to repeat overall modernization during the remainder of the facility's operational lifetime by ensuring that a smooth migration/upgrade path for the system is possible and can be conducted in manageable steps. In such a way, the shorter life cycles of digital I&C can be addressed while the possibility to further implement advanced techniques or applications in the system remains feasible. Here the project manager and/or the decision makers can end up in a conflict that originates from the requirements of perhaps many different authorities to keep the facility's I&C equipment state of the art, while maximizing the benefit of proven operational experience and technological maturity. Given a long remaining lifetime for operational I&C systems (those not important to safety and not requiring licensing approvals), there is a tendency towards the use of new products with an associated lack of available operational experience and increased risk of being subject to problems due to lack of their being tested. At a minimum, the core of the system infrastructure has to be long lived. Given a short remaining lifetime, an older, more mature platform may be used if the supply of spare parts and support can be ensured for the remaining operational life of the facility.

For modernization projects, another important decision in the basic planning is to select and define the scope of the project. Perhaps the easiest solution is to plan for equivalent functionality, but it is advisable to also consider the introduction of new or improved functionality. The final decision depends on several contributing factors such as the original design of the facility, its remaining lifetime, operational experience and regulatory requirements. The potential for facility life extension must also be considered when classifying the remaining facility lifetime. Regardless of the type of modernization, there

are always certain basic considerations to be kept in mind before the start of the project. Typical considerations are:

— Licensing (regulator involvement);
— Performance/scale effects/expansion capability;
— Upgrade capability;
— Defence in depth;
— Redundancy/diversity;
— Availability/reliability;
— Interfaces between the existing and new I&C, introduction of smart field instrumentation;
— Human factors engineering (HFE).

To establish the scope of the modernization project, a number of general considerations must be taken into account which could affect the implementation of the I&C installation. These include:

— Availability of power supplies and power supply distribution.
— Use of existing cabling.
— Heating, ventilation and air conditioning heat loads in locations where equipment will be located.
— The physical space available for locating new equipment during the installation phase and final operation.
— Training for engineers and technicians involved in the design, testing, and installation and commissioning phases. These may be the same people as those responsible for the operation and maintenance of the system.
— The suitability of existing sensors and actuators, and their potential compatibility with a new digital control system.
— Requirements for computer security to protect the system from unauthorized use and to protect any sensitive data on the system.
— Documentation for obtaining regulatory approval.
— Whether or not the project can be managed by internal facility staff or if an expert consultant or contractor is required to be engaged.

In the case of partial I&C modernization, HSI aspects must be considered early in the project as it is the interface between the existing and new parts of a control room or control location. This may have an influence on the boundaries of the modernization steps due to requirements originating from the operator's tasks. If not properly accounted for at the beginning, it may be difficult, costly, or impossible to comply with these requirements later in the project.

Analysis of industry best practices allows the design team to see what is available on the market and being used by other research reactors. Pre-existing solutions and products may be used to reduce cost and risk, since novel or new designs tend to introduce risk into a project.

Once the analysis of solutions and products has been conducted, conceptual designs can be proposed. This activity allows the project team to conceptualize the required system so that solutions can be qualitatively compared, and the best solution can be chosen.

Cost is an important factor at the feasibility stage. Once the conceptual designs are complete an estimate of cost can be made. When the best conceptual design has been chosen a project budget can be estimated. A project plan completes the feasibility phase and allows the project to progress to the requirement specification phase.

4.2.2. Requirement specification phase

When the scope of the project has been determined, the requirements to be placed on the new I&C system have to be defined. These requirements are typically derived from many sources such as regulatory requirements, process requirements, industrial standards and facility requirements. Since most systematic errors are introduced in the I&C systems during the requirement specification phase, it is advisable to use some kind of formal method for managing the specification.

An overall requirement specification for the entire stepwise modernization process must be prepared which accounts for the basic concepts defined in the preliminary planning and design phase. This specification must define the intended scope of the project regardless of the intended implementation schedule. While the specification defines the intended number of modernization steps, with their respective scopes and boundaries together with the most probable sequence of the modernization steps, the number (and therefore the scope) and sequence of the modernization steps may change in the future due to new or modified general conditions. The scope must list all systems and functions with their current classification/categorization and a new classification/categorization, if applicable (i.e. the modernization results in a change in classification).

The overall requirement specification must define the major requirements of the I&C system for the entire project in sufficient detail, such as response time, accuracy and requirements for deterministic behaviour. This must also include the requirements for communication interfaces with existing systems and future third party systems, if necessary. For existing communication interfaces, all existing information must be presented in the overall requirement specification. Furthermore, requirements on HFE for the HSI have to be specified in terms of

operational safety, security and ergonomics. It is advisable to develop at least a preliminary plan which deals with the stepwise transformation of the control room and control locations (from conventional (analog) to hybrid (analog and digital) or to a mostly digital control room).

If the I&C system is not being installed with a uniform and homogeneous platform, it is very important to consider the needs of the operational staff in the control room, and to provide clear and unambiguous displays of the necessary information to safely and efficiently monitor and control the facility, especially during unplanned events. When using different I&C systems (each with its own HSI), the standardization of symbols, colours, icons and other items for graphic displays is highly recommended. Alternatively, applying a common platform for operation and monitoring (e.g. a supervisory control and data acquisition system) with different systems or components at the process level may be considered.

4.2.3. Contractual arrangements

Contractual arrangements are to be determined by the facility owner early in the project. These may be considered after the feasibility or requirements specification phases, once the project scope is defined. A number of different options must be considered, depending on the level of internal expertise and availability of resources. The owner may choose to engage an independent consultant to act on the owner's behalf for the design and implementation phases of the project if expert internal resources are not available. Consultants must have expert knowledge in the field of nuclear and/or industrial control systems and work with the owner on the particular requirements of the research reactor. The facility owner may choose to complete all design phases and then issue a tender for a system supplier. A third option is to choose the system vendor early in the project and include the design phases in their scope of supply.

The structure of the system supply contract may vary. For example, the system vendor may be contracted to supply all hardware and software and for all installation work. This means that the vendor will control all subcontractors employed for support work such as cabling and power supply installation. Alternatively, work could be separated such that the owner takes control of all support systems installation in preparation for the arrival of the system vendor.

When negotiating contract conditions for the project, arrangements for unforeseen costs must be described. During the project, extra costs may be incurred for changes resulting from licensing or the requirements of safety authorities. Typically, a schedule of rates may be specified so that the contractor is paid by the hour for the extra work required.

The contract must include the conditions for a defects liability period, where the contractor is required to rectify any faults and provide support to the

owner. The supply of spare parts must also be incorporated in the scope of the contract so that the owner is prepared for routine operation when the project is completed. Each alternative must be assessed for risk and cost, considering the vendor's capabilities, internal resource constraints and any physical or computer security concerns.

4.2.4. Preliminary design phase

The preliminary design activity represents the delineation of a specific implementation solution to fulfil the facility I&C needs. During the preliminary design phase, the system architecture is selected and system requirements are allocated to hardware, software components and to personnel. The activities conducted during the preliminary design include requirements specification analysis, system description and preliminary design review (PDR). The guidelines mentioned in the Appendix, especially IAEA Safety Standards Series Nos SSR-3 [5] and SSG-37 [6], can be considered at this early stage of the design process.

It is customary for the responsibility for performing the preliminary design to reside with the main consultant/contractor, taking into account the functional baseline requirements prepared by the facility operator during the conceptual design phase. The facility operator's role in this phase involves supervision, reviewing and supporting the consultant/contractor.

4.2.4.1. Requirements specification analysis

During this stage, the intended use of the system to be developed must be analysed to specify the system requirements. The specifications must describe:

— Functions and capabilities of the I&C system;
— Organizational and user requirements;
— Safety requirements;
— Security requirements;
— HFE (ergonomics);
— Interface requirements;
— Operation and maintenance requirements;
— Design constraints and qualification requirements.

The outcome of the analysis is the preparation of the I&C requirements specification document.

Preliminary design starts with the functional baseline, defined during the requirements specification phase, and continues with analysis of system

level functional requirements to translate them into design requirements for the different subsystems that will constitute the I&C system. The requirement specification analysis is a continuation of the analysis started in the requirements specification phase and will define specific requirements for the hardware, software, and personnel responsible for the development of the I&C system.

If a consultant or contractor is engaged to perform the requirement specification analysis, the main sources of information required to be supplied are:

— Request for tender specification;
— Contract and subcontract specifications;
— Process control requirements;
— Applicable standards;
— Technical specification outcome from consultant/contractor site visit and preliminary evaluation;
— Environmental, safety and regulatory constraints.

In this case, the responsibility of the facility owner is to ensure that all the information from the requirements specification is included in these documents. Alternatively, the requirements specification analysis may be conducted internally by the facility owner.

The requirement specification analysis process starts with a review of these documents and collates all the requirements from the system level to the subsystems level until all functions, parameters and interfaces have been identified, which allows the design to meet all the original facility's requirements. The level of detail of the analysis is such that it allows the designers to completely define the major subsystems comprising the I&C system.

4.2.4.2. System description

During the requirements specification analysis process, the system specification activities begin where the system design translates from the functional to the physical design. This activity performs the transition from what the system needs to do to how it is going to do it. The system specification outcome is used to procure or design and develop the major components of the system and subsystems.

4.2.4.3. System overall architecture design

The main objective of the system architecture design phase is to establish the high level topology of the system. The architecture design phase must identify

items of hardware, software, and manual operations. It is necessary to ensure that all the system requirements derived from the requirement analysis are allocated among the items. The system architecture, hardware and software components, including the system requirements allocated to the items, must be described in the system architecture design document. The system hardware architecture must also be documented schematically, showing all major components:

> "The inputs to the design process for the instrumentation and control system architecture should refer to the documents on the safety design basis for the facility, which should provide [the information stated in Section 3.16 of IAEA SSG-37] [6]".

4.2.4.4. Requirements allocation and subsystems or components specification

Requirements allocation, during the preliminary design phase, refers to the process of grouping or combining similar functions and systems requirements, based on a preliminary architecture of the system. System requirements must be allocated to lower level components based on functionality and system analyses. Usually, the requirements allocation is an iterative process with the requirements analysis.

Grouping similar functions assists in the determination of the major subsystems and components that are required to form the system. The aim of this activity is to carry out the translation from functional design to physical design.

Each subsystem or component that has to perform the assigned group function is normally referred to as a configuration item (CI). The CIs represent hardware, software, or a combination of both that fulfils the allocated group of functions and requirements. The requirements allocation describes exactly what each CI needs to do in terms of function and performance.

The requirements allocation in the preliminary design process assigns the functions and requirements to a set of major CIs. Each CI can then be managed individually as a separate item and is depicted in more detail during the detail design phase.

The higher level requirements and the derived requirements for each CI will form the basis of the technical specification for that CI. This specification is usually named a subsystem or component datasheet specification.

4.2.4.5. Interface identification and design

During the definition of the system architecture and the selection of the CIs that cover the system, the interfaces between the CIs are also identified. Identification of interfaces is a critical part of the preliminary design because

these determine the successful operation of the system, once integrated, and sets restrictions and requirements on the CI design.

The task of integrating different system elements is managed primarily through a document called the interface control document, which contains sufficient detail to completely define the interfaces between the different subsystems. The interface control document contains various types of information, depending on the nature of the interface. Examples of some of the different types of interfaces are electronic, electrical, hydraulic/pneumatic, environmental, physical, computer network and software.

4.2.4.6. Selecting the preferred solution

After the allocation of requirements, the activities can concentrate on the consideration and evaluation of the alternatives among the available COTS products, modified COTS and customized items for development. The analysis is a trade off between factors and capabilities, such as product reliability and availability, delivery time, technology, openness, compliance with market standards, involved risks (including regulatory risk) expected maintainability and future upgrades and support. An evaluation of the vendor's computer security program and its effectiveness needs to be considered, especially for COTS.

Preliminary design activities are conducted to ensure that the design satisfies the functional groupings. The design engineers, at this stage, begin to consider the selection of the major subsystems and components derived from the requirement allocation in the CIs, in order to fulfil the specified level of the requirements.

Once the preliminary design process is developed, the result is a preliminary architecture made up of various units and components comprising hardware, software and HSI. Each subsystem has an individual description of its intended purpose and the requirements specification that it has to satisfy. These individual specifications have to be detailed enough for hardware engineers to design and build the equipment, if required, and for software engineers to specify the general functionality of the software.

4.2.4.7. Preliminary design review

The PDR is aimed at ensuring the adequacy of the preliminary design effort prior to allowing the design focus to shift to detailed design. It is designed to assess the technical adequacy of the proposed solution in terms of technical risk and the likely satisfaction of the functional baseline. It also investigates the identification of subsystem interfaces and the compatibility of each of the CIs.

The PDR must be conducted only when the facility owner is satisfied that the system design has progressed enough to justify holding the design review. Prior to the commencement of the PDR, it is necessary for the system architecture to be delineated with all CIs identified and documented.

The major task during the PDR is to verify that all the system level requirements are satisfied. In addition, the PDR has to provide a check of the results of the requirements analysis, the requirements allocation process, and the evaluation studies conducted during the architecture definition. If any deviation from the requirements is found during the PDR review, it must be noted, and a corrective action be determined.

The following activities are performed in the PDR process:

— Evaluation of the preliminary design to examine, in detail, the design activities to ensure that they have been properly conducted;
— Approval of all specifications following a formal review process;
— Approval of interface control documents following a formal review process;
— Assessment of traceability through a review to ensure that all the requirements in the conceptual design have been adequately captured and addressed;
— Assessment of supporting documentation with a review of additional documentation like as test plans, basic engineering drawings and manufacturing plans.

4.2.5. Detailed design phase

The detailed design phase is undertaken after approval of the PDR which validates the preliminary design phase activities. The detailed design phase follows the development effort to specify and describe all components of the system in detail. The main design activities comprise the following:

— Preparing a description of lower level components making up the subsystems, including hardware, software, and HSI and their interrelationships;
— Defining the characteristics of these component items through specifications and design data;
— Finalizing the design of all interfaces necessary to support system integration;
— Procuring specifications for the above component items whether they are COTS equipment or custom designed if they are unique to the system under development;
— Developing a prototype or engineering models of the critical parts of the system for testing and evaluation, if required;
— Redesigning work, if it is required, after prototype testing and evaluation;

— Conducting a critical design review (CDR) to ensure that the design is ready for construction and operation.

4.2.5.1. Detailed requirements specification

Detailed design requirements have to be derived from the system specification developed during the feasibility design, and the analysis in the requirements specification derived during the preliminary design phase. The requirements specifications contain the requirements, and appropriate specifications and characteristics, that have to be incorporated into the design of specific components. Also, the specifications have to include the descriptions of the requirements (functional, technical, and performance) for the interfaces relevant to the subsystems and components.

The specification process is responsible for establishing requirements at each level in the system's hierarchical design structure. The process evolves through iterations of analysis, synthesis, and evaluation until the definition of all system components is complete. It is essential that for each I&C system, subsystem and component the specification includes the following details:

— Safety and the relationship with safety issues;
— Control/logic algorithms;
— Alarms and warning list, together with the alarm management strategy;
— Operational procedures;
— HSI and ergonomics;
— System interfaces.

4.2.5.2. Detailed design process

The detailed design process is initiated by the completion of the previous phases in the system specification and the set of specifications provided in the preliminary design phase. The designers are able to determine the detailed design and definition of the subsystems and components using these requirements. The design engineers must, at this point, use design tools such as trade off analyses to determine the best way to fulfil all the detailed requirements specification.

Typically, the detailed design process is iterative in nature and is dominated by reviews and feedback at each stage. The subsystem definitions are then further analysed and broken down into lower level portions of the design that include assemblies, units, components, and parts. These low level definitions are then reviewed to ensure that the definitions are complete and meet the overall system requirements.

The review process ensures that this process is complete and accurate before the design effort focuses on component purchasing and system construction and production. The documented items for this design phase include, but are not limited to, the following engineering specifications:

— Detailed system description;
— Components list (system, subsystem and component level);
— Components description;
— Piping and instrumentation diagrams (with complete instrumentation details);
— Input/output points list;
— Interconnection drawings (specific connections between racks and cabinets);
— Loop diagrams;
— Cable list;
— Data sheets;
— HSI specification;
— Set point calculations;
— Software description in terms of functional block diagrams;
— Qualification plan;
— Factory acceptance tests (FAT) plan;
— Startup procedures;
— Procurement specification;
— Failure modes and effects analysis (for safety systems).

The design has now reached a stage where each hardware and software component has been designed completely, as well as the interfaces between the system components and between the external systems. The individual items can now be procured, modified, or constructed in the case of custom development items.

4.2.5.3. Qualification process

The nuclear industry has become a relatively small market for vendors of nuclear grade equipment and components, with a decreasing number of suppliers leading to the increased costs of nuclear grade equipment. As a result, it has become common for facility operators to purchase lower cost and widely used COTS equipment and to qualify them for use in safety systems by performing facility specific qualification analysis and testing. Alternatively, for I&C system equipment and software purchased as nuclear qualified, a quality assurance programme is still required to ensure that the design and development processes are controlled and monitored and that V&V activities are completed.

In general, replacement COTS equipment can be used in nuclear research reactor facilities in non-safety grade applications if it meets the facility performance standards. These standards are usually satisfied by choosing proven commercially available items that are widely used and have an acceptable performance record in similar applications, although perhaps in other industries.

However, in applications where performance can affect nuclear safety and the facility licensing basis, a higher standard has to be met, and the regulatory authorities have to be satisfied that the performance and quality of a given item are compatible with the conditions of the licence. For these applications, an agreed method is needed for assessing and qualifying the items for their intended service. Therefore, it is necessary to establish a qualification plan during the detailed design phase.

As an example, the following standards could be used to develop a plant specific equivalent qualification process:

(a) IEEE standards:
   — IEEE 344, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Station (relevant sections to be adapted for research reactors) [16].

(b) IEC standards:
   — IEC 60780-323, Qualification of Electrical Equipment of the Safety System for NPPs [17]. Note that this incorporates IEEE 323.
   — IEC 60880, Software for Computers in the Safety Systems of NPPs [18].
   — IEC 61226, Classification of I&C Systems Important for Safety for NPP [19].

The qualification process must enable the qualification of equipment for use in the particular facility undergoing the modernization project. The development and implementation of this process will allow the purchase of non-nuclear qualification COTS equipment which is then subject to the tests and analysis required for granting equivalent qualification.

4.2.5.4. Factory acceptance test plan

During the detailed design phase, the test and evaluation activities will reach a critical stage, and the strategies, procedures, and support needed to perform comprehensive tests and evaluations have to be determined.

One of the major project milestones in the testing process is the factory acceptance test (FAT), and at the end of detailed design phase a detailed FAT plan must be established. The FAT activity is a hold point which requires the

approval of the operator before all the system components can be shipped to the installation site or accepted for installation. The test must be conducted at the site of the system vendor but may be arranged at the facility, space allowing, for smaller projects and this may be preferred from a security aspect. It must include all system communications, HSI level hardware and software, control algorithms, field inputs and outputs, system security and critical system interfaces. FAT provides a good opportunity for the facility operators, technicians and engineers to be exposed to the final design and to provide feedback to designers. However, it is advisable to involve regulatory authorities in the FAT.

4.2.5.5. Critical design review

The CDR is the final design review prior to the official acceptance of the design and the subsequent commencement of construction and production activities. The result of successful completion of the CDR is the establishment of the product baseline, which effectively freezes the design. At this point changes in the system design must come only from the discrepancies identified during testing activities or as a result of regulatory review.

Some integration and prototyping will have occurred since the last review (PDR), and the CDR investigates and assesses the success of this effort as a key indicator of design maturity. A CDR is required to be conducted on all the components of the system (hardware and software) to demonstrate that the components under review satisfy the functional and performance requirements allocated to them in the product specifications, and their compatibility with other parts of the system, including other equipment, facilities, and personnel. The CDR is also the time in which plans for construction and production of the system are evaluated and approved.

Examples of documentation that would be expected to be reviewed prior to the CDR include revised design specifications, system hardware and software specifications, interface documentation, test and evaluation procedures, relevant technical data including assembly diagrams and drawings, installation drawings and schematics and software application specifications.

Following the completed CDR, any departures from the approved design must be noted and corrective action defined, although at this stage in the project any major departures are normally difficult to rectify, incurring costs and delays. The aims of the CDR must include the following:

(a) Evaluation of the detailed design: A great deal of effort has been put into establishing the detailed design of the system prior to this phase. The design is documented in various forms including the detailed product specifications and related engineering drawings. The CDR must evaluate

this documentation set and the detailed design to ensure that they adequately address the original requirements. It is necessary to ensure that any discrepancies raised during the PDR have been rectified adequately.

(b) Determination of readiness for manufacturing/construction: In addition to the product specifications, the interface control documents and the drawings, the CDR must review the manufacturing plan and the quality assurance plans to ensure that the detailed design for the hardware items can progress to construction and installation. The system prototype (if produced) provides an excellent tool for assessing readiness for construction and production.

(c) Determination of the maturity of the software: Software will need to enter the coding stage following the CDR (this can be considered the software equivalent of hardware fabrication). The software product specifications (including interface requirements and design) must be thoroughly reviewed prior to approving the software aspects of the CDR.

(d) Determination of design compatibility: The CDR must investigate and confirm design compatibility of components items with other aspects of the system or facility. This requires a detailed investigation of all external and internal interfaces. The system prototype will provide an indication of design compatibility.

(e) Establishment of the product baseline: The complete set of product specifications, once approved, will form the initial product baseline for the system. Functional and physical configuration audits must eventually be conducted prior to the formal approval of the product baseline for a system.

4.2.6. Implementation phase

This phase includes the realization of the different components of the I&C system and the associated V&V activities. The realization tasks deal with pre-existing and new hardware and software components. The inputs of this phase are the detailed hardware and software subsystems and components specifications including the reliability assessment. The outputs are:

— The manufacture or procurement of hardware.
— The development of new system software if COTS system software is not available for the facility. Normally, very few new software developments are required and generic software components are used.
— The development or generation of the application software components by programming or parameterizing software tools. It is common to reuse generic software components, for the same equipment types, to generate application software code from the software specification. Requirements for software development are given in IEC 60880 [17] and IEC 62138 [20], and

IEC 60987 [21] for hardware. Requirements for computer security are given in Ref. [1].

4.2.7. Integration and testing phase

4.2.7.1. Factory acceptance testing

The first step in this phase is to execute the unit tests on each component. Following this, the testing must require assembly of the hardware and software modules (project specific applications and parameterizing generic modules) and verification of compatibility of the software loaded into the hardware platform. Facility computer security risk management and system computer security risk management must also be verified at this stage [1].

The performance requirements have to be verified when all the application software (either developed from the vendor engineering tools or specifically developed) has been integrated in the system. In the integration phase, there have to be the following:

(a) Test cases which demonstrate that each selected application function performs its task.
(b) Configuration control, which must be applied to:
    — Changes in platform (due to ongoing development by the supplier);
    — Changes in design (applications);
    — Changes in configuration;
    — Changes in tuning parameters.

Special attention must be given to interfaces with proprietary non-standard communication protocols. The main input document for this stage is the FAT plan and the main output document is the FAT report accepted by the operator.

In addition to the FAT, the facility owner may choose to further test system integration in the case where more than one system is connected in the final installation. The purpose of this additional test is to ensure that the communication links between systems operate reliably and with high availability.

4.2.7.2. Installation in a simulated environment

In a large and stepwise modernization project, it is important that the core system, in its original configuration, be tested in a staging area before implementation in the facility. This is because some tests (control of performances in abnormal configurations, for example) may not be easily performed in the

facility environment. In this case, the FAT must include this additional validation stage in a simulated environment.

A facility training simulator, if available, could be used after project completion as a test bed for validation of new applications or modifications and for operator training prior to implementation in the facility.

4.2.8. Installation and commissioning phase

The installation and commissioning phase is required to ensure that the system is installed and started according to the design requirements and performs the tasks described in the system requirements specification. The main issues to consider are:

— The entire system has to be checked, including the field devices.
— There must be detailed installation, commissioning, and testing documents outlining each procedure to be carried out.
— Completed checks must be signed off in writing, documenting that each function has been checked and has satisfactorily passed all tests.
— The installation plan has to consider the benefits and risks of gradual installation over several routine facility shutdowns or extending one shutdown to complete the entire project work. There may be a need to return to the original system, in part because operation of the facility may be compromised by an installation problem.

4.2.8.1. Installation

The project's installation activities include installation of sensors, final control elements, field wiring, junction boxes, cabinets, logic system, operator interface(s) and alarm panels, and other hardware associated with the I&C system. During the installation of the system it is advantageous to consider the following:

— For consistency, it is recommended that all installation work be completed by the same contractor and workforce, which must include the instrument and electrical work.
— Ensuring that the design package given to the contractor is complete and accurate. The training and experience of the contractor is important.
— All devices must be installed per the manufacturer's recommendations.
— All equipment and installations have to comply with code and statutory requirements in effect at the local site. The contractor has to understand these requirements and ensure compliance.

— All materials supplied by the contractor must be of suitable quality for the intended service. Detailed specifications for these items must always be established.
— All devices must be installed in a manner that allows easy access for maintenance and testing. Specifications must be developed to give guidance to the contractor.
— All instruments have to be calibrated prior to installation or in situ, if possible. Certified calibration documentation has to be provided. The installation contractor must not make any changes to the calibration or settings of the field devices unless specifically requested.
— Care is needed to protect all field devices from physical and/or environmental damage prior to installation.
— The contractor must not make any changes or deviations from the design drawings without written approval. Management of change procedures has to be followed, and changes must be recorded on a set of as-built drawings.

4.2.8.2. Installation checks

Installation checks ensure that the system and all components are installed in agreement with the detailed design and are ready for validation. The activities confirm that the equipment and wiring are properly installed, and the field devices are operational. The installation checks are best completed by separating the work into two distinct phases:

(a) *Field device and wiring check:* This is a check on how the field devices are physically installed, including the wiring, wiring continuity, terminations, earthing, tagging and junction boxes. The installation contractor usually completes this phase with no power to the system.
(b) *Device functional check:* This is a check of the field devices and the logic system after the different system units are powered. The installation contractor or an independent crew may complete this phase.

These checks are intended to confirm that:

— Power sources are operational;
— All instruments have been properly calibrated;
— Field devices are operational;
— The loops are operational.

Once the contractor is satisfied that the system installation is complete, an inspection must be conducted jointly by the owner and contractor. Any required

corrective actions must be documented and agreed between the inspection parties and rechecked following the completion of any rectification work.

4.2.8.3. Site acceptance testing

Validation of the I&C system is commonly referred to as a site acceptance test (SAT). These checks must only be done after the installation checks have been finished and all corrective actions completed. The main objective of validation is to confirm that the system meets the original requirements specified, including the correct functionality of the system logic.

The SAT must also ensure that:

— All equipment has been installed as per the vendor's installation instructions;
— A test plan is available with procedures for testing and documenting results;
— All safety life cycle documents are complete.

Validation activities may include, but not be limited to, checks that prove:

— The system performs under normal and abnormal operating modes (e.g. start up, shutdown and maintenance);
— Integrated I&C systems (e.g. the reactor protection system and control systems) are communicating properly;
— The sensors, logic, control algorithms, and final elements perform in accordance with the safety and control requirement specification;
— The sensors activate at the set points defined in the requirement specification;
— Confirmation that functions perform as specified on invalid process variables (e.g. out of range);
— The proper control, interlock and shutdown sequences are activated;
— The I&C system provides the proper annunciation and operational displays;
— Algorithms and computations are accurate;
— Total and partial reset function, and bypass reset functions operate as designed;
— Manual actions and shutdown functions operate as designed;
— Diagnostic functions perform as required;
— Test intervals are documented in maintenance procedures consistent with the safety integrity level (SIL) requirements;
— I&C system documentation is consistent with actual installation and operating procedures.

As in the case with FAT, it is advisable that the facility's regulator be invited to participate in key aspects of the SAT.

4.2.8.4. Required documentation for SAT

The documentation needed to support the validation depends upon the complexity of the system and the documents originally prepared by the design team. Detailed SAT procedures must be prepared and followed. The following documentation is usually required to support the validation of the SAT:

— Validation checkout procedures;
— Control and safety requirement specification;
— Test case procedures;
— Architecture diagram;
— Complete list of inputs and outputs with physical addresses;
— Piping and instrument diagrams;
— Specification sheets (data sheets) for all major equipment, including manufacturer, model and options;
— Loop diagrams;
— Electrical schematics;
— Logic diagrams (for example, cause and effect or Boolean diagrams);
— Floor plans showing the locations of all major equipment;
— Junction box and cabinet connection diagrams;
— Drawings to indicate interconnections and terminations of all wires;
— Calibration certificates and check sheets;
— Vendor equipment documentation, including specifications, installation requirements, and operating and engineering manuals.

4.2.8.5. Commissioning phase

The commissioning tests involve the functional tests of the system connected to the facility processes and the other I&C systems. It includes final operational testing, tuning of process parameters, and validation of the long term performance of the system. The safety aspects of the commissioning phase for research reactors are considered in IAEA Safety Standards Series No. NS-G-4.1, Commissioning of Research Reactors [22] and the security aspects in IAEA Nuclear Security Series No. NSS 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [1].

The commissioning phase contains several steps. During the execution of these steps, the licensing authority will review the actual tests and results before allowing the owner to proceed further. Commissioning test results form a major part in the licensing authority's final approval of the new I&C system or its modernization.

The procedure for the complete commissioning of the upgraded I&C system must include instructions for a progressive activation of the connections to each facility system or subsystem. The control of the commissioning process must be formally documented, including a list of detailed tests. In the case of a modernization project, a comparison of the commissioning results with baseline data has to be performed and any deviations have to be explained.

For modernization projects, commissioning must be planned in detail, must immediately follow any partial installation and must be scheduled for completion within routine facility shutdowns (e.g. those for refuelling and maintenance work). Detailed commissioning test instructions for each equipment and application must also be provided.

For new facilities, commissioning must be planned so that the main infrastructure of the system is tested, after which the connections to the process systems are conducted. Planning the commissioning of these connections is dependent on the installation and commissioning activities for the individual process systems. Before starting the commissioning phase all facility field instruments have to be calibrated according to manufacturer's or internal specifications and the corresponding certificates issued.

4.2.9. Handover phase

4.2.9.1. Training

Training has to be carefully planned and adapted for the different users in the facility, primarily the operation and maintenance staff. Training must start before implementation of the new system in the facility. Maintenance and facility engineering personnel must be involved in the system design as early as possible and must participate in the engineering activities and FAT activities to acquire the appropriate knowledge. The training of the operation personnel must be in phases, starting with basic training for handling the HSI, leading up to comprehensive training of the new HSI. This training must, if feasible, be performed before the FAT and be used as an additional activity to validate the new system. All negative findings must be carefully analysed, and the necessary corrective actions and improvements must be implemented in the system. After any corrective work, the FAT must be repeated, and a second round of training must be executed before implementation is scheduled to occur.

4.2.9.2. Operation and maintenance

The possibility of I&C specific operational acceptance testing is often limited and depends on the shutdown and startup programme of the facility. The

contractual warranty period may take effect after the system is handed over to the owner. In addition, the owner will now be responsible for configuration control and change management. This is an important aspect of all design work. Loss of configuration control during a project can result in large schedule delays and cost impacts and a reduced ability to maintain the required quality of a project. Loss of an installed and operating system due to maintenance activities or modifications could cause the system to be considered functionally inoperative and put the facility into a limiting condition, action statement or requiring immediate shutdown. Configuration control is required throughout the entire life cycle of the facility, from the first design concept to the last upgrade or modification prior to the end of the facility's life. Change management is the methodology used to maintain the configuration control of design changes at any time during or after a project. Change management controls the quality process of design changes so that they are performed in a clear, methodical manner.

The process for change management is part of the facility's quality system or high quality and properly documented results. Change management and configuration control together ensure that a system, and any changes made to that system, will be maintained and/or performed to sufficient quality standards that are traceable and compliant with all required documentation.

Routine maintenance activities for the I&C system must be identified during the planning phases to ensure that the system is prepared for handover. The considerations for maintenance must include budgeting for operating costs and future system upgrades. These maintenance activities include:

— Software backups;
— Archiving historical data;
— Routine analysis of system error and operational logs;
— Cabinet and hardware inspections;
— System upgrade life cycle reviews;
— Security software updates;
— Workstation management;
— Power supply hardware maintenance;
— Sensor calibrations.

4.3. LICENSING PROCESS

4.3.1. General principle for licensing

The licensing process has to follow the facility's national regulations. In practice, there may be considerable differences between countries in how the

licensing process must be structured. The most significant difference in the regulation may be the need for prior approval, if a large modification is proposed to be undertaken. In some countries, even the smallest changes to safety systems are required to be pre-approved by the licensing authority. The licensing plan may be based on a hierarchical approval process, where the licensee has to apply to the authority for approval or release of each phase in the modernization project, for example, feasibility, design, installation and commissioning. More generally, the requirement is that any modification to safety, or safety related systems, will require regulatory approval.

In the licensing process, the regulator may ask for evidence of development excellence which might consist of issues such as: maturity of the design and implementation organization, methodologies and tools used in processes and programmes, and demonstrated rigour in the development process, including those for both the hardware and software. For COTS products this may be difficult to demonstrate. This information would be used in establishing regulatory confidence in the development process. The licensing efforts will be heavily dependent on the safety classification and therefore the classification will be one of the most important factors during the licensing process. There are several approaches offered to a licensee and a regulator for the demonstration of the safety of a computer based system [21, 23]. Depending on national regulations, the emphasis may vary between the following approaches to licensing:

— Based on deterministic arguments;
— Rule based (based on norms and standards);
— Based on technical assessment;
— Claim and evidence based;
— Risk based.

In some cases, there is a system history available from the use of the platform and the software applications in other countries. In these cases, the question is if, and to what extent, the licensing experience is applicable. In many countries, there is interest from the regulatory body when there is a change in the HSI with a possible influence on operator performance and HFE. The most significant regulatory issues concern the possibility of increasing human error rates to errors in advanced operator support systems. Examples of regulatory concerns with HSI can be found in Ref. [11].

4.3.2. Plan for the licensing process

When the dialogue has been established between the licensee and the regulator, they must agree on a plan for the licensing process. It is also important

that the vendor is briefed on this subject, to understand the licensing process for the country in question. For modernization projects the plan could be divided into different subplans such as:

— Requirement specification;
— Design and implementation plan;
— Functional designs;
— Control room modification plan;
— Documentation plan;
— Installation and commissioning plan.

Basic issues that have to be discussed during the licensing process include the following:

(a) Regulatory requirements to be applied: Requirements may not be fully developed, especially for digital I&C, which means that an iterative process has to be applied. In addition, new requirements, for example, as provided by new or revised guidelines and standards, may have to be considered.
(b) Agreements on safety demonstrations: The licensing plan must identify how the safety demonstration will be achieved. More precisely, the plan must identify requirements, the types of evidence that will be used, and how and when this evidence must be produced.
(c) The need for diversity, redundancy and independence: The licensee and regulator must formulate and agree upon the specification of DECs. This includes addressing where in the primary protection system a full defence against potential CCFs is required and where it is not. Relaxation in the requirements for a full defence against CCFs may, in some cases, be justified by probabilistic arguments.
(d) Protection philosophy: Identifying those safety functions that cannot be diverted to backup systems and where diversity is needed. If possible, there must be a prior agreement on specific requirements that may have to be in place for the implementation of these functions.
(e) Documentation: Identifying which documents and when they have to be submitted for regulatory review. Necessary hold points, where a regulatory acceptance is needed before the modernization project can proceed, must be defined in advance. Depending on the regulatory body sometimes lengthy delays during this process lead to project delays, so it is extremely important to discuss the schedule of all submittals well in advance with the regulator.

Computer security could also be a licensing requirement for reactors with the potential to cause unacceptable radiological consequences (sabotage) using either LEU or HEU.

4.3.3. Major phases in the licensing process

The phases in the licensing process typically follow the phases of the system requirements and design process. This means that it is a good practice for the regulator to independently review the outputs of each stage. In principle, these reviews can be seen as verification steps aimed at building confidence. However, they must not be regarded as partial approvals that would commit the regulator to an approval of the final product. Hold points during the project implementation phase have to be considered and agreed. In the licensing process the following typical regulatory aspects have to be considered:

— Scope, categorization, safety classification and system definition;
— Safety analysis;
— Quality assurance/quality control;
— Engineering process;
— Strategies and plans;
— Assumptions, preconditions, design basis and requirements;
— Regulations, codes, standards and guidelines;
— System architecture and functional system detailed design;
— HFE, main control room, and HSI;
— V&V and testing of facility I&C;
— Product platform qualification;
— Installation and integration in plant;
— Facility documentation;
— Organization and competence assurance;
— Operation, maintenance and modifications.

4.3.4. The safety case

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

The safety case for licensing of digital I&C equipment must describe the safety philosophy, the basic safety principles involved and how the I&C equipment complies with these principles. Further, the safety function of the

system has to be clearly defined and its importance documented, including the scope and functions of the I&C system and its connection to the overall process. In doing so, the classification of the equipment must be established based on IAEA, IEC, IEEE or other recognized classification guidelines. The safety case must include descriptions of system requirements and specifications and outline all quality assurance and V&V steps that will be taken. The scope and depth of the V&V must be explained, together with acceptance criteria for the results of testing activities. In particular, the requirements for acceptability of the I&C system must be clearly expressed together with the justification for acceptability. The safety case, included in the SAR, becomes a living document which forms part of the facility license and, as such, it has to be kept up to date throughout the I&C system's life cycle.

4.4. NEW FACILITIES

I&C projects in new research reactor facilities essentially have the same phases during the life cycle process as modernization projects of existing facilities. The main differences in this case lie in the fact that there are no restrictions imposed by an existing facility, such as physical space and already established control processes. The design process of I&C systems could be efficiently harmonized with the rest of the facility, more easily to fulfil all requirements of current applicable standards, and make use of the state of the art technologies that provide enhanced features, as well as increased reliability and availability.

The projects for new facilities may have different requirements compared with a modernization project in an existing facility where:

— Regulator review and approval are required for all I&C systems;
— More attention and project team interaction are required to design the I&C for new process systems;
— More reporting to various levels of project management would be required to ensure that project coordination is controlled between various engineering disciplines;
— The I&C team needs to coordinate with process system teams for installation and commissioning activities.

The I&C system of a new nuclear research reactor or irradiation facility is designed and implemented in close relationship with the design and implementation of process systems and major facility components to ensure that all requirements placed on process equipment are accurately reflected.

It is essential to determine the requirements of I&C systems in the context of the overall facility goals, objectives, and commitments. This process must include determining all the features of the I&C systems and the control room of the new facility.

INTRODUCTION TO THE SUPPLEMENTARY FILES

The on-line supplementary files for this publication, which can be found on the publication's individual web page at www.iaea.org/publications, contain examples of new and upgraded digital I&C projects conducted at different research reactors. These contributions provide a variety of project descriptions and concentrate on different aspects of the projects. The IAEA is not responsible for the content of the Member State reports, and all questions must be directed to the individual authors or organizations.

Appendix

RELATED PUBLICATIONS

The standards and regulation followed for the implementation and licensing of digital I&C systems in research reactors vary from country to country. Owners must always conduct a thorough review of current Member State standards and regulations that are applicable, review international standards and obtain further insight from the experience of others with a similar reactor design.

Table 2 provides a list of selected IAEA and international standards and publications related to digital I&C implementation. The information in these publications must be tailored to suit the requirements of the research reactor considering a modernization project. As most of these documents are specific to nuclear power plants, the requirements may be more than what is required for a research reactor [2].

TABLE 2. SELECTED PUBLICATIONS RELATED TO THE IMPLEMENTATION AND LICENSING OF DIGITAL I&C SYSTEMS

Organization	Publication	Publication title	Year of publication
EC	EUR 19265	Common Position of European Nuclear Regulators for the Licensing of Safety Critical Software for Nuclear Reactors	2000
EPRI	EPRI TR-102348	Guidelines on Licensing Digital Upgrades	2002
IAEA	TECDOC-1016	Modernization of Instrumentation and Control in Nuclear Power Plants	1998
IAEA	TECDOC-1066	Specification of Requirements for Upgrades Using Digital Instrument and Control Systems	1999
IAEA	Technical Reports Series No. 384	Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control	1999

TABLE 2. SELECTED PUBLICATIONS RELATED TO THE IMPLEMENTATION AND LICENSING OF DIGITAL I&C SYSTEMS (cont.)

Organization	Publication	Publication title	Year of publication
IAEA	Technical Reports Series No. 387	Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook	1999
IAEA	TECDOC-1147	Management of Ageing of I&C Equipment in Nuclear Power Plants	2000
IAEA	Technical Reports Series No. 397	Quality Assurance for Software Important to Safety	2000
IAEA	NS-G-2.3	Modifications to Nuclear Power Plants	2001
IAEA	TECDOC-1226	Managing Change in Nuclear Facilities	2001
IAEA	TECDOC-1327	Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants	2002
IAEA	INSAG-19	Maintaining the Design Integrity of Nuclear Installations throughout Their Operating Life	2003
IAEA	TECDOC-1335	Configuration Management in Nuclear Power Plants	2003
IAEA	TECDOC-1389	Managing Modernization of Nuclear Power Plant Instrumentation and Control Systems	2004
IAEA	TECDOC-1500	Guidelines for Upgrade and Modernization of Nuclear Power Plant Training Simulators	2006
IAEA	NS-G-4.1	Commissioning of Research Reactors	2006

TABLE 2. SELECTED PUBLICATIONS RELATED TO THE IMPLEMENTATION AND LICENSING OF DIGITAL I&C SYSTEMS (cont.)

Organization	Publication	Publication title	Year of publication
IAEA	Safety Reports Series No. 55	Safety Analysis for Research Reactors	2008
IAEA	NP-T-1.4	Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants	2009
IAEA	NP-T-1.5	Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants	2009
IAEA	Safety Standards Series No. SSG-2	Deterministic Safety Analysis for Nuclear Power Plants	2010
IAEA	Nuclear Security Series No. 17	Computer Security at Nuclear Facilities	2011
IAEA	Nuclear Security Series No. 33-T	Computer Security of Instrumentation and Control Systems at Nuclear Facilities	2018
IAEA	Safety Standards Series No. SSG-22	Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors	2012
IAEA	Safety Standards Series No. SSG-24	Safety in the Utilization and Modification of Research Reactors	2012
IAEA	Safety Standards Series No. SSG-37	Instrumentation and Control Systems and Software Important to Safety for Research Reactors	2015
IAEA	Safety Standards Series No. SSG-39	Design of Instrumentation and Control Systems for Nuclear Power Plants	2016
IAEA	Safety Standards Series No. SSR-2/1 Rev.1	Safety of Nuclear Power Plant: Design	2016

TABLE 2. SELECTED PUBLICATIONS RELATED TO THE IMPLEMENTATION AND LICENSING OF DIGITAL I&C SYSTEMS (cont.)

Organization	Publication	Publication title	Year of publication
IAEA	Safety Standards Series No. GSR Part 4/Rev.1	Safety Assessment for Facilities and Activities	2016
IAEA	Safety Standards Series No. SSR-3	Safety of Research Reactors	2016
IAEA	TECDOC-1830	On-line Monitoring of Instrumentation in Research Reactors	2017
IEC	IEC 61131-3	Programmable Controllers — Part 3, Programming Languages	2003
IEC	IEC 62138	Nuclear Power Plants — Instrumentation and Control Important to Safety: Software Aspects for Computer-based Systems Performing Category B or C Functions	2004
IEC	IEC 60987	Nuclear Power Plant Instrumentation and Control Important to Safety — Hardware Design Requirements for Computer-Based Systems	2007
IEC	IEC 61226	Nuclear Power Plants — Instrumentation and Control Important to Safety: Classification of Instrumentation and Control Functions	2009
IEC	IEC 60880	Nuclear Power Plants — Instrumentation and Control Systems Important to Safety: Software Aspects for Computer-based Systems Performing Category A Functions	2010

TABLE 2. SELECTED PUBLICATIONS RELATED TO THE IMPLEMENTATION AND LICENSING OF DIGITAL I&C SYSTEMS (cont.)

Organization	Publication	Publication title	Year of publication
IEC	IEC 61508	Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems	2010
IEC	IEC 61513	Nuclear Power Plants — Instrumentation and Control Systems Important to Safety: General Requirements for Systems	2011
IEC	IEC 60780-323	Nuclear Facilities — Electrical Equipment Important to Safety: Qualification *Note that this incorporates and supersedes IEEE-323*	2016
IEC	IEC 62645	Nuclear Power Plants — Instrumentation and Control Systems: Requirements for Security Programmes for Computer-based Systems	2014
IEC	IEC 62859	Nuclear Power Plants — Instrumentation and Control Systems: Requirements for Coordinating Safety and Cybersecurity	2016
IEEE	IEEE-279	Criteria for Protection Systems for Nuclear Power Generating Stations	1971
IEEE	IEEE-1008	Standard for Software Unit Testing	1987
IEEE	IEEE-830	Recommended Practice for Software Requirements Specification	1998
IEEE	IEEE-829	Standard for Software Test Documentation	2008

TABLE 2. SELECTED PUBLICATIONS RELATED TO THE IMPLEMENTATION AND LICENSING OF DIGITAL I&C SYSTEMS (cont.)

Organization	Publication	Publication title	Year of publication
IEEE	IEEE-1028	Standard for Software Review and Audits	2008
IEEE	IEEE-603	Standard Criteria for Safety Systems for Nuclear Power Generating Stations	2009
IEEE	IEEE-828	Standard for Software Configuration Management Plans	2012
IEEE	IEEE-338	Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Stations Safety Systems	2012
IEEE	IEEE-1012	Standard for Software Verification and Validation Plans	2012
IEEE	IEEE 7-4.3.2	Standard Criteria for Digital Computers in Safety Systems	2016

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. NSS 33-T, IAEA, Vienna (2018).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of New and Existing Research Reactor Facilities in Relation to External Events, Safety Reports Series No. 41, IAEA, Vienna (2005).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety in the Utilization and Modification of Research Reactors, IAEA Safety Standards Series No. SSG-24, IAEA, Vienna (2012).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. SSR-3, IAEA, Vienna (2016).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[8] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[9] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev 1, INSAG-12, IAEA, Vienna (1999).

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2002).

[12] NUCLEAR REGULATORY COMMISSION, Human–System Interface Design Review Guidelines Rev. 2, Rep. NUREG-0700, NRC, Washington, DC (2002).

[13] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rep. NUREG-0800, NRC, Washington, DC (2019).

[14] NUCLEAR REGULATORY COMMISSION, Human Factors Engineering Program Review Model Rev. 2, Rep. NUREG-0711, NRC, Washington, DC (2004).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Analysis for Research Reactors, Safety Reports Series No. 55, IAEA, Vienna (2008).

[16] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, Recommended for Seismic Qualification of Class 1E Equipment for nuclear Power Generating Stations, Rep. IEEE 344, IEEE, Piscataway, NJ (2004).
[17] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Electrical Equipment of the Safety System: Qualification, Rep. IEC-60780, IEC, Geneva (1998).
[18] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety: Software Aspects for Computer-based Systems Performing Category A Functions, Rep. IEC-60880, IEC, Geneva (2010).
[19] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety: Classification of Instrumentation and Control Functions, Rep. IEC-61226, IEC, Geneva (2009).
[20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety: Software Aspects for Computer-based Systems Performing Category B Functions, Rep. IEC-62138, IEC, Geneva (2004).
[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety: Hardware Aspects for Computer-based Systems, Rep. IEC-60987, IEC, Geneva (2007).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Commissioning of Research Reactors, IAEA Safety Standards Series No. NS-G-4.1, IAEA, Vienna (2006).
[23] COURTOIS, P.J., A Framework for the Dependability of Computer Based Systems. Summary in CEMSIS: Cost Effective Modernization of Systems Important to Safety, Pre-proceedings of FISA-2003, EU Research in Reactor Safety, Rep. EUR-20281, Luxembourg (10–13 November 2003) 301–305. Available at https://www.info.ucl.ac.be/~courtois/.

ABBREVIATIONS

CCF	common cause failure
CDR	critical design review
CI	configuration item
COTS	commercial off the shelf
DEC	design extension condition
FAT	factory acceptance test
HEU	high enriched uranium
HFE	human factors engineering
HSI	human–system interface
IEEE	Institute of Electrical and Electronics Engineers
LEU	low enriched uranium
PDR	preliminary design review
PIE	postulated initiating event
SAT	site acceptance testing
SSC	structures, systems and components
V&V	verification and validation

CONTRIBUTORS TO DRAFTING AND REVIEW

Ampong, A.G.	Ghana Atomic Energy Commission, Ghana
Amponsah-Abu, E.O.	Ghana Atomic Energy Commission, Ghana
Anandapadmanaban, B.	Indira Gandhi Centre for Atomic Research, India
Avila, A.	INVAP S.E., Argentina
Bae, S.H.	Korea Atomic Energy Research Institute, Republic of Korea
Benitez, J.	Instituto Nacional de Investigaciones Nucleares, Mexico
Bickford, G.	University of Florida, United States of America
Borio di Tigliole, A.	International Atomic Energy Agency
Cagnazzo, M.	University of Pavia, Italy
Carvalho, P.V.	Instituto de Engenharia Nuclear, Brazil
Celis Del Angel, L.	Instituto Nacional de Investigaciones Nucleares, Mexico
Cho, Y.G.	International Atomic Energy Agency
Ciobanu, D.	Institute for Nuclear Research, Romania
Delbianco, D.	INVAP S.E., Argentina
El-Koliel, M.S.	Atomic Energy Authority, Egypt
Emi-Reynolds, B.	Ghana Atomic Energy Commission, Ghana
Evangelos, M.	National Center of Scientific Research, Greece
Ezati, A.	Atomic Energy Organization of Iran, Islamic Republic of Iran
Flego, C.	Australian Nuclear Science and Technology Organisation, Australia
Gasu, P.D.	Ghana Atomic Energy Commission, Ghana

Gbadago, J.K.	Ghana Atomic Energy Commission, Ghana
González, J.L.	Instituto Nacional de Investigaciones Nucleares, Mexico
Gruia, L.	Institute for Nuclear Research, Romania
Haggag, S.	Atomic Energy Authority, Egypt
Iqbal, M.	PINSTECH, Pakistan
Jinchuk. D.	Independent consultant, Argentina
Jordan, K.A.	University of Florida, United States of America
Karla, M.	Bhabha Atomic Research Centre, India
Kim, J.H.	RTP Korea, Inc., Republic of Korea
Kim, Y.K.	Korea Atomic Energy Research Institute, Republic of Korea
Klevtsov, O.	State Scientific and Technical Center for Nuclear and Radiation Safety, Ukraine
Kochova, M.	dataPartner s.r.o. Czech Republic
Korovikov, A.	National Nuclear Center of the Republic of Kazakhstan, Kazakhstan
Kropik, M.	Czech Technical University, Czech Republic
Lewis, J.	University of Florida, United States of America
Linn, M.A.	Oak Ridge National Laboratory, United States of America
Magrotti, G.	University of Pavia, Italy
Manera, S.	University of Pavia, Italy
Maslina, M.I.	Malaysian Nuclear Agency, Malaysia
Messai, A.	Commissariat à l'énergie atomique, Algeria
Mocanasu, M.	Institute for Nuclear Research, Romania
Morris, C.R.	International Atomic Energy Agency

Musitelli, G.	University of Pavia, Italy
Nardò, R.	University of Pavia, Italy
Obeng, H.	Ghana Atomic Energy Commission, Ghana
Oberholtzer, H.H.	Oak Ridge National Laboratory, United States of America
Palacios, J.	Instituto Nacional de Investigaciones Nucleares, Mexico
Park, K.Y.	Korea Atomic Energy Research Institute, Republic of Korea
Pulpa, A.	Institute for Nuclear Research, Romania
Qadir, J.	PINSTECH, Pakistan
Qaiser, S.H.	PINSTECH, Pakistan
Radu, G.	Institute for Nuclear Research, Romania
Rao, D.V.	International Atomic Energy Agency
Rataj, J.	Czech Technical University, Czech Republic
Rivero, T.	Instituto Nacional de Investigaciones Nucleares, Mexico
Sainz, E.	Instituto Nacional de Investigaciones Nucleares, Mexico
Salam, M.	Atomic Energy Commission, Bangladesh
Salvini, A.	University of Pavia, Italy
Sengupta, C.	Bhabha Atomic Research Centre, India
Serrao, B.	Amazul S.A, Brazil
Sharma, R.	International Atomic Energy Agency
Shaw, K.L.	Oak Ridge National Laboratory, United States of America
Shim, S.	International Atomic Energy Agency

Shokr, A.	International Atomic Energy Agency
Sklenka, L.	Czech Technical University, Czech Republic
Sridhar, S.	Indira Gandhi Centre for Atomic Research, India
Velasco, A.E.	Australian Nuclear Science and Technology Organisation, Australia
Veramendi, L.E.	Peruvian Institute of Nuclear Energy, Peru
Vinolia, K.	Indira Gandhi Centre for Atomic Research, India
Wetchagarun, S.	Thailand Institute of Nuclear Technology, Thailand
Wijtsma, F.	Pallas Reactor, Netherlands
Witkowsky, T.	National Center for Nuclear Research, Poland
Zaikin, A.	JSC “SNIIP-Systematom”, Russian Federation

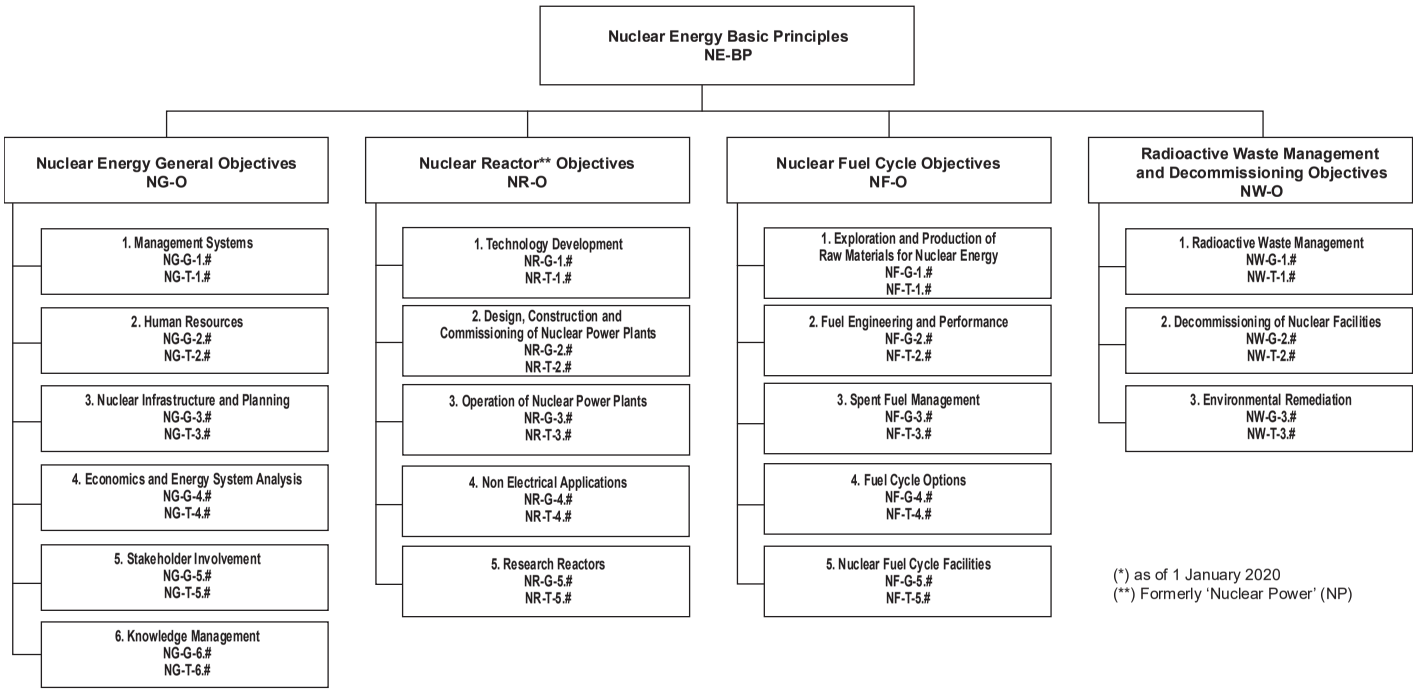
Consultants Meeting

Vienna, Austria: 7–11 March 2011

Technical Meetings

Vienna, Austria: 14–18 May 2012, 3–7 July 2017, 1–5 July 2019

Structure of the IAEA Nuclear Energy Series*



(*) as of 1 January 2020
(**) Formerly 'Nuclear Power' (NP)

Key

BP: Basic Principles
O: Objectives
G: Guides and Methodologies
T: Technical Reports
Nos 1–6: Topic designations
#: Guide or Report number

Examples

NG-G-3.1: Nuclear Energy General (**NG**), Guides and Methodologies (**G**), Nuclear Infrastructure and Planning (topic **3**), **#1**

NR-T-5.4: Nuclear Reactors (**NR**)*, Technical Report (**T**), Research Reactors (topic **5**), **#4**

NF-T-3.6: Nuclear Fuel (**NF**), Technical Report (**T**), Spent Fuel Management (topic **3**), **#6**

NW-G-1.1: Radioactive Waste Management and Decommissioning (**NW**), Guides and Methodologies (**G**), Radioactive Waste Management (topic **1**) **#1**

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

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

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA