IAEA-TECDOC-1662/Rev.1

IAEA TECDOC SERIES

IAEA-TECDOC-1662/Rev.1

# Preparing and Conducting Review Missions of Instrumentation and Control Systems in Nuclear Power Plants

IAEA
International Atomic Energy Agency

# PREPARING AND CONDUCTING REVIEW MISSIONS OF INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
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-TECDOC-1662/REV. 1

# PREPARING AND CONDUCTING REVIEW MISSIONS OF INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

## COPYRIGHT NOTICE



For further information on this publication, please contact:

Nulear Power Engineering Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org


Printed by the IAEA in Austria
July 2016

**IAEA Library Cataloguing in Publication Data**

Names: International Atomic Energy Agency.
Title: Preparing and conducting review missions of instrumentation and control systems in nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2016. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1662/rev. 1 | Includes bibliographical references.
Identifiers: IAEAL 16-01053 | ISBN 978–92–0–105816–4 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Control rooms. | Nuclear power plants — Instruments. | Nuclear reactors — Control..

## FOREWORD

The mission for Independent Engineering Review of Instrumentation and Control Systems (IERICS) in nuclear power plants was established with the aim of conducting peer reviews of instrumentation and control (I&C) design documents, implementation processes, prototype I&C systems and actual systems already deployed in operating nuclear power plants.

Organizations in Member States, such as nuclear utilities, regulators, designers, vendors and technical support organizations can benefit from I&C technical reviews by requesting IERICS missions, which provide a detailed technical assessment on I&C systems, as well as recommendations for improvement.

The IERICS mission is conducted by a team of international subject matter experts from various complementary technical areas. The review is based on appropriate IAEA publications, such as safety guides and technical reports, and the mission's findings are summarized in a report, including a list of recommendations, suggestions and identified good practices.

The review is not intended to be a regulatory inspection or an audit against international codes and standards. Rather, it is a peer review aimed at improving design and implementation procedures through an exchange of technical experiences and practices at the working level. The IERICS mission is applicable at any stages of the life cycle of I&C systems in nuclear power plants, and it is initiated based on a formal request through official governmental and IAEA channels from an organization in a Member State.

The formation of the IERICS mission is based on the recommendation of the IAEA Technical Working Group on Nuclear Power Plant Instrumentation and Control (TWG-NPPIC). The recommendation came from the recognition that the IAEA can play an important role in the independent assessment and review of NPP I&C systems in terms of their compliance with IAEA safety guides and technical documents.

This publication is a revision of IAEA-TECDOC-1662, which was published in 2011. It has been revised by international experts who participated in previous IERICS missions, and reflects experiences and lessons learned from the preparation and conduct of those missions. The IAEA officer responsible for this publication was J. Eiler of the Division of Nuclear Power.

*EDITORIAL NOTE*

*This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.*

*Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.*

*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 publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.*

# CONTENTS

# 1. INTRODUCTION

## 1.1. BACKGROUND

The review mission titled 'Independent Engineering Review of Instrumentation and Control Systems' (IERICS) was established in 2009 with the aim of conducting peer reviews of instrumentation and control (I&C) design documents, prototype I&C systems, and actual systems already deployed in operating nuclear power plants (NPP). The IERICS mission is performed by a group of invited subject matter experts from various IAEA Member States. The mission is based on available IAEA and other documents, and on recommendable practices as represented by the expertise of the review team. Its findings are summarized in a mission report, including a list of recommendations, suggestions, and identified good practices.

The assessment provided in the mission report, describing issues and good practices, represents the opinion of the expert team, and does not constitute recommendations or suggestions made by the IAEA or made on the basis of a consensus of IAEA Member States.

The guidelines for organizing and conducting an IERICS mission are laid down in this publication.

## 1.2. OBJECTIVE

The IERICS mission is a comprehensive engineering review service directly addressing strategy and the key elements for implementation of modern I&C systems, noting in applicable cases specific concerns related to the implementation of digital I&C systems and the use of software and/or digital logic in safety applications of a NPP.

The IERICS mission is conducted by a team of international experts with direct experience applicable to the areas of review. Judgements of compliance are made on the basis of IAEA publications (mainly IAEA Safety Guide SSG–39 [1], but also the other references of this publication [2-15]), and of the combined expertise of the international review team.

The key objectives of the IERICS mission are to:

—Assess the design approach, principles and procedures of the system under review;
—Identify existing or potential design, operational and licensing related issues or concerns of the system under review;
—Propose measures to address issues identified;
—Identify any outstanding good practice that could be a benefit to other organizations;
—Facilitate exchange of experience.

In order to fulfil these objectives, the IERICS mission aims to:

—Provide the counterpart (the organization that has requested the IERICS mission and the beneficiary of the review mission) with an objective opinion, with respect to international standards and practices, of the design and design practices related to the system under review;
—Provide the counterpart with recommendations and suggestions for improvement in areas where the design or performance may appear to fall short of recognized international good practices;
—Provide key staff at the counterpart with an opportunity to discuss their practices with experts who have experience of other practices in the same field;

—Provide the counterpart with recognition of their good practices identified during the course of the review;

—Provide experts of the counterpart, expert reviewers from Member States and the IAEA staff with opportunities to broaden their experience and knowledge of their own field.

The counterpart is not necessarily an I&C system or platform designer. It could be a general plant designer, an NPP undergoing modernization, or a Nuclear Energy Programme Implementing Organization (NEPIO) from a newcomer country, when any of these wants an independent expert opinion on the I&C that is proposed to them. It may then define the scope of the mission, and require the concerned I&C suppliers to provide the information, documentation and support necessary to the review. This might be particularly interesting for NEPIOs, which can then benefit from the collective experience of the IERICS team.

One important constraint is that the I&C systems or platforms to be reviewed should have reached a maturity level where sufficiently detailed and stable information is available for the review. Systems still in early development stages would not be good candidates for an IERICS mission.

The findings of the review are associated with specific system designs and product versions as identified in the scope of the review. In principle, these findings are not applicable to subsequent changes and modifications to the systems; hence, the validity of the report will be lost as changes occur. The counterpart might elect to request additional reviews to update the report findings and maintain its validity.

## 1.3. SCOPE

The scope of the IERICS mission is determined based on a mutual agreement between the IERICS team leader and the counterpart. It is normally defined during the preparatory phase of the mission (see Section 2.2.). A reasonable portion of non-safety I&C systems may be included in the scope of the IERICS mission in order to give a more balanced overview of the entire plant I&C architecture. For such systems, the general recommendations of SSG–39 [1] will be used as a reference, when applicable.

The scope of the mission specifies the range of the systems to be reviewed (e.g. a complete I&C architecture, particular I&C systems, or I&C platforms), their precise identification (e.g. names and version numbers), their boundaries, their positions and roles in the overall I&C architecture, their safety classifications and their main missions. It also specifies the properties to be reviewed, and the review basis and reference documents to be used for the review. It should also state the extent of the counterpart's role and the limits of its responsibilities, so that the IERICS team can adjust the review to those aspects that are or should be under counterpart's control.

An IERICS mission is limited to the technical, engineering and safety aspects of the NPP's I&C architecture and systems, unless there is a specific request for addressing additional areas, such as issues related to the overall NPP plant safety case, human factors, etc.

These guidelines provide a basic structure and common reference across the various areas covered by an IERICS mission. The report describes in detail all steps and processes that should be followed during the preparation, implementation and closing phases of the review mission by the IERICS team members and the counterpart. Publications referenced in these guidelines [1-15] could provide additional useful information for the counterpart while preparing for the IERICS mission. A template for the mission report is also given in Appendix II.

The guidelines are intended to help IERICS team members formulate their review in conjunction with their own experience. They should not be considered exhaustive and should not limit the reviewer's investigations, but rather should be considered as illustrative of the comprehensive requirements according to which the review is carried out. Reviewers should keep in mind that it is practically impossible, in the timeframe of a review mission, to cover the entire scope of a given section of the guidelines to the same level of detail. Therefore, it is expected that, based on the review of the advance information package (AIP) prepared by the counterpart, the reviewers will apply their judgement to decide which topics need more in-depth evaluation during the review.

On the counterpart side, the potential organizations requesting the IERICS mission could be:

—Nuclear utilities;
—Nuclear regulators and government authorities;
—Decision makers (authorities and utilities);
—Research, development and technical support organizations;
—Vendors and manufacturers.

## 1.4. STRUCTURE

Section 2 provides guidelines regarding the overall organization of the IERICS mission, from the preparatory phase to follow-up missions.

Section 3 provides guidelines regarding the principles and techniques to be applied in the course of an IERICS mission. There may be some overlap in the recommendations of Sections 2 and 3, so that each section can be read on its own.

The References section provides a set of references that may be used for an IERICS mission.

Appendix I provides a list of technical topics that could be considered when defining the scope of a specific IERICS mission. It can be used as a discussion tool with the counterpart.

Appendix II provides a mission report template, including templates for issue sheets and good practice sheets.

The two Appendices are also available in electronic form for preparation of the specific mission reports by the IERICS team.

# 2. ORGANIZATION OF THE IERICS MISSION

## 2.1. OVERVIEW OF THE IERICS PROCESS

An IERICS mission is initiated based on a formal request through official IAEA and governmental channels of a Member State from an organization (e.g. nuclear utility, regulatory authority, technical support organization, design organization, or vendor). The actions prior to this request are not the object of, and are not discussed in, this guideline. Throughout this guideline, the specific organization that is responsible to answer the requests and questions of the IERICS team is designated as the counterpart. The IERICS related activities are based on the following:

- Documentation describing the design and design basis of the I&C system under review including, but not limited to, documentation demonstrating how the system supports the overall plant safety case.
- Interview and discussions with staff of the counterpart.
- Written procedures and methods associated with the design, verification, validation, testing, installation, maintenance and commissioning of the system under review.
- Written documentation related to the qualification of structures, systems and components selected for use in the system under review.
- Observations of demonstrations of operation and / or maintenance activities of portions of the systems in a plant or representative test facility.

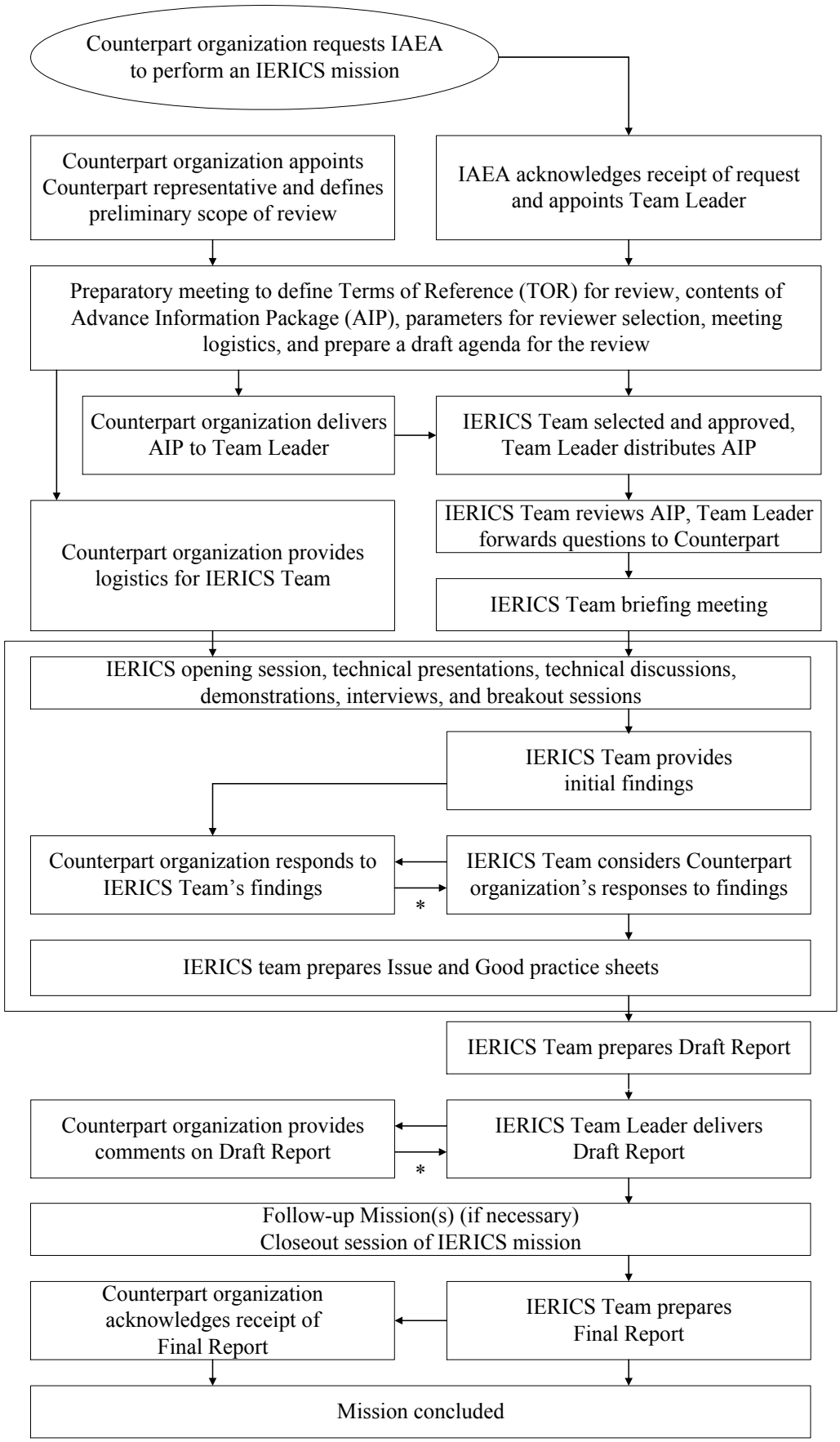
The review focuses on technical areas, related regulatory requirements, the managerial aspects of policy implementation, the control/coordination of related activities, continuous review and improvement of activities, as well as document control.

It is important to note that an IERICS mission is a flexible service and the review areas and the depth of the review can be tailored according to the request of the counterpart and agreed during the preparation for the review. However, the scope of the mission should be limited to technical, safety and procedural aspects. Commercial, business development and marketing interests shall be excluded from the review scope.

The IERICS process may be divided into three main phases, each with its own purpose and goals:

- The preparatory phase, which also includes a formal meeting between members of the IAEA staff and the counterpart staff, and is called the preparatory meeting;
- The main review phase, which consists essentially of a review mission;
- The follow-up phase, which may include optional follow-up missions.

Figure 1 provides an overview of the various tasks associated with an IERICS mission.




* Resolution of the findings and of the draft report may require multiple cycles

*FIG. 1. Overview of an IERICS mission.*

## 2.2. PREPARATORY PHASE AND PREPARATORY MEETING

Preparation is the key element for the success of an IERICS mission. The objective of the preparatory phase is to address a number of topics, mainly:

- The appointment of the IERICS team leader and identification of the counterpart representative;
- The clarification of the objectives and scope of the specific mission;
- The selection of the IERICS team members;
- The establishment of the review mission agenda;
- The documents to be provided to the IERICS team members prior to the review mission, i.e. the terms of reference and the advance information package;
- The establishment of a code of conduct to be applied by the IERICS team;
- The resolution of logistics issues (e.g. transportation, lodging, payment, insurance, meeting rooms) for the review mission;
- The establishment and signature of non-disclosure agreements;
- The measures to be taken to address possible language barriers (i.e. translation of review materials and/or translation services during the review mission);
- The selection of specific codes, guides and standards to be applied during the review mission.

Preparation should begin no later than eight months prior to the review mission. This will enable each participant (from the IERICS team and from the counterpart) to plan for specific activities and to conduct the necessary research and study prior to the review mission.

### 2.2.1. Appointment of the IERICS team leader

After a mission request for an IERICS mission from an organization of a Member State has been received by the IAEA, the IAEA will designate a staff member (expert in I&C) of the Division of Nuclear Power of the Department of Nuclear Energy as the IERICS team leader. At the same time, the counterpart is requested to designate a contact person, the counterpart representative, with whom the IERICS team leader may directly correspond. All subsequent activities of the IERICS mission will be under the leadership and responsibility of these two individuals.

In particular, the IERICS team leader is responsible for all preparatory activities, acts as an official liaison with the counterpart organization, co-chairs the review mission with the counterpart representative, coordinates the preparation and issuance of the mission report and is responsible for all follow-up activities.

### 2.2.2. Objectives and scope of the specific IERICS mission

The scope of an IERICS mission identifies what is to be reviewed. This could be a single item, or multiple items. An item to be reviewed can be:

- An I&C architecture;
- An I&C system;
- An I&C platform.

The exact objectives and scope of the specific IERICS mission need to be stated precisely, based on the IERICS mission request. These should clearly identify:

- Background information on why the IERICS mission has been requested and what its expectations are;
- The platforms or systems to be reviewed (hereafter designated as the system under review), including its main components, their version designation, the system boundaries, interfaces and environment;
- The system functions, properties and features to be assessed by the review;
- The review basis and reference documents against which the system under review will be assessed. These should usually include any relevant IAEA Safety Guides, IAEA Nuclear Energy Series and IAEA Technical Reports. Other documents describing recognized international good practices, such as IEC standards or IEEE documents may be listed. The review basis needs to be precisely defined in the preparatory meeting.

Table 1 below indicates which SSG–39 [1] sections are likely to be relevant for I&C system, platform and complete architecture reviews, respectively.

TABLE 1. TYPICAL SAFETY GUIDE REQUIREMENTS FOR DIFFERENT REVIEW ITEMS

| SSG–39 section | I&C system | I&C platform | I&C architecture |
|---|---|---|---|
| 2. Management system for I&C design | Y | Y | Y |
| 3. Design basis for I&C systems | Y | | Y |
| 4. I&C architecture | Y (4.13) | Y (4.12) | Y |
| 5. Safety classification of I&C functions, systems and equipment | Y | | Y |
| 6. General recommendations for all I&C systems important to safety | Y | Y | |
| 7. Design guidelines for specific I&C systems and equipment | Case by case | Case by case | |
| 8. Considerations relating to the human-machine interface | If a control room system | | Y |
| 9. Software | If digital | If digital | |

The review of systems or platforms might need to consider some architectural aspects (SSG–39 [1], section 4).

From the perspective of the counterpart organization, it may be appropriate to include a reasonable portion of non-safety I&C systems in the scope of the IERICS mission in order to give a more balanced overview of the entire plant I&C architecture.

### 2.2.3. Selection of the IERICS team members

The IERICS team is composed of the IERICS team leader and typically four to six additional team members. A deputy team leader may be appointed if necessary. The typical team composition includes a majority of external senior experts and one or two IAEA staff members (the team leader and the deputy team leader if applicable). In case the scope of the mission includes safety related areas, the appropriate sections of the IAEA Department of Nuclear Safety and Security will be consulted on the selection of the team members.

The composition and size of the team will usually depend on many factors, such as:

- The competences needed for the review. These competences may be identified based on the main characteristics (e.g. technologies, architecture) of the system, on the system properties and features to be assessed, and on the selected review basis and reference.
- The estimated volume of work for the review mission, based on a breakdown of the work to be performed during the review mission into well-defined technical sessions.
- The need to represent a wide scope of international practices. To this end, the team members should represent a variety of national approaches to I&C design and design processes. Team member should have, in addition to their particular area of expertise, knowledge of some other national approaches and some other relevant areas. Coupling this knowledge with the IAEA safety standards and other IAEA guidance publications allows good international practices to be identified.
- In some cases, the need to overcome possible language and/or cultural barriers. In such cases, a team member familiar with the language and culture of the counterpart organization may be of great benefit to the review as a whole.
- The need to avoid conflicts of interest with the counterpart. The selection of team members should consider their impartiality and the relationship of team members' organizations to that of the counterpart. In particular, reviewers from the counterpart and dependent organizations should not be included in the IERICS team. Also, reviewers from organizations considered to be competitors to the counterpart's organization may be excluded from the review team.
- The possible need of security vetting. Access to certain facilities and information may require security vetting to be carried out on the IERICS review team. The responsibility for identifying the vetting requirements that allow such access to be granted lies with the counterpart. The responsibility for providing the information to satisfy these requirements lies with the IERICS team leader and team members. The counterpart is subsequently responsible for handling the information provided and to ensure that the vetting process is completed prior to the review mission.

The selection of the team members is under the responsibility of the IERICS team leader, but the list of team members should be submitted to the counterpart for approval.

The IERICS team members are responsible for preparing for the mission by studying relevant information provided by the counterpart in the advance information package (but not limited to this), preparing plans of their review and formulating questions and comments prior to commencing the mission.

If the IERICS team leader and the counterpart agree, observers can join the review team. Normally an observer is either an IAEA staff member who needs to be trained for subsequent IERICS missions, or a person from an organization that is going to request a mission. The observers may assist the IERICS team during the review mission. They are subject to the same rules and constraints (e.g. code of conduct, nondisclosure agreement) as the IERICS

team members, but their participation should financially be covered by their own organizations.

The IERICS team members should also provide feedback on the application of the IAEA safety guides (e.g. which parts need to be updated, what issues could not be referenced to the standards).

### 2.2.4. Review mission agenda

The review mission should be conducted following a review mission agenda. This is a key element for the good implementation of the review mission, as it will be the basis for:

—Estimating the necessary competences and resources, both for the IERICS team and for the counterpart;
—Determining whether the objectives and scope of the IERICS mission are compatible with the available resources and time schedule;
—Other aspects of the preparation phase, such as the preparation of presentations and information packages by the counterpart and the preparation of logistic aspects (e.g. meeting rooms, technical visits).

The agenda would typically make provision and plan for different types of work sessions:

—The briefing meeting for the IERICS team, to make sure that all team members have the required background information;
—A plenary opening session, where the IERICS team and the counterpart introduce one another and present a reminder of the objectives and scope of the IERICS review and of the mission;
—Several technical sessions, where the IERICS team and the counterpart discuss the technical aspects of the system under review; different subtypes of technical sessions may be identified, such as:
  - Technical presentations, where the counterpart presents aspects of the system to the IERICS team;
  - Technical visits that allow the IERICS team to collect facts on the ground that may be otherwise difficult to determine from the documentation and/or presentations;
  - Focused reviews that allow the IERICS team to study some selected topics in deep detail.
—IERICS team meetings described in Section 2.3.8;
—A plenary closeout session, where the IERICS team presents its findings, the counterpart expresses their point of view and the IERICS team adjusts its findings as appropriate;
—The debriefing meeting (involving only the IERICS team members), where a quasi-final state for the mission report is completed.

Section 2.3 provides specific guidelines for each of these work session types. Hereafter are a few general suggestions pertaining to the review mission agenda:

—The development and modification of the review mission agenda needs a close cooperation between, and the agreement of, the IERICS team leader and the counterpart representative, as both sides will need to do extensive preparation prior to the mission.

—A technical session may be a plenary session (i.e. involving the complete IERICS team) or a breakout session (i.e. involving only a part of the IERICS team). Plenary sessions facilitate the sharing of information within the team. Breakout sessions optimize the use of the team resources when many subjects need to be covered, or when the team members have very different and exclusive competencies. It is usually the responsibility of the IERICS team leader to decide which subjects will need to be covered by plenary sessions, and which by breakout sessions.

—Enough time needs to be devoted to IERICS team meetings, so that the findings and conclusions of the review are those of the team, and not only of individual team members. They should be held at the end of each day. They may be rather short the first days, but as the review mission gets closer to the closeout session, more time is necessary to harmonize viewpoints and finalize the findings list.

—Enough time should be given to the counterpart to provide adequate answers, but the counterpart should anticipate that issues will arise and should have adequate resources and competences available to respond rapidly.

### 2.2.5. Terms of reference

During the preparatory phase, the IERICS team leader should prepare a draft terms of reference for the IERICS mission. This should be discussed and agreed with the counterpart during the preparatory meeting. The terms of reference should contain the following items:

—Background information;
—Objectives and scope of the review;
—Date and place for the review;
—Names of IERICS team leader and counterpart representative;
—Review basis and reference;
—Review subjects (the system under review);
—The need for IAEA involvement.

### 2.2.6. Advance information package

The advance information package (AIP) is the set of documents that the counterpart makes available to the IERICS team members during the preparatory phase. It should be written in English, taking into consideration the fact that the IERICS team members have no prior knowledge on, and have never seen, the systems to be reviewed, and will have to understand the systems to be reviewed only based on the AIP. Also, they usually have no precise knowledge of the counterpart's national practice and regulations.

A clear and precise AIP can save time and effort and helps avoid unnecessary questions. It should cover only the systems to be reviewed; the systems not under review should be included only to clarify their connections and interactions with the systems to be reviewed. In order to facilitate both the development of the AIP by the counterpart and its review and analysis by the IERICS team, it is suggested to proceed in two steps.

*First step*

The objective of the first step is to provide an introduction to the systems to be reviewed: their nature (e.g. a complete I&C architecture, particular operational systems, or I&C platforms), their precise identification (e.g. names and version numbers), their positions and

roles in the overall I&C architecture, their boundaries, their relationships and connections with other systems and equipment, their safety classifications, their operation and main functions, etc.

The information provided by the counterpart could be presented in the spirit and supported by diagram(s) in the style of Fig. 2, where levels of defence in depth are represented as vertical columns and I&C layers (e.g. instrumentation, priority logic / signal conditioning, automatic functions, human system interfaces, etc.) are represented as horizontal lines. The precise organisation of the I&C architecture into levels of defence in depth and I&C layers is the counterpart's design choice, but the role of each line and column should be clarified. A given system (or the systems that would typically be implemented with a platform to be reviewed) would lie at an intersection.

The diagram(s) should also represent the connections of the systems to be reviewed with other systems, the safety class of each represented system, and whether for a given system a communication link is input only, output only, or input and output.

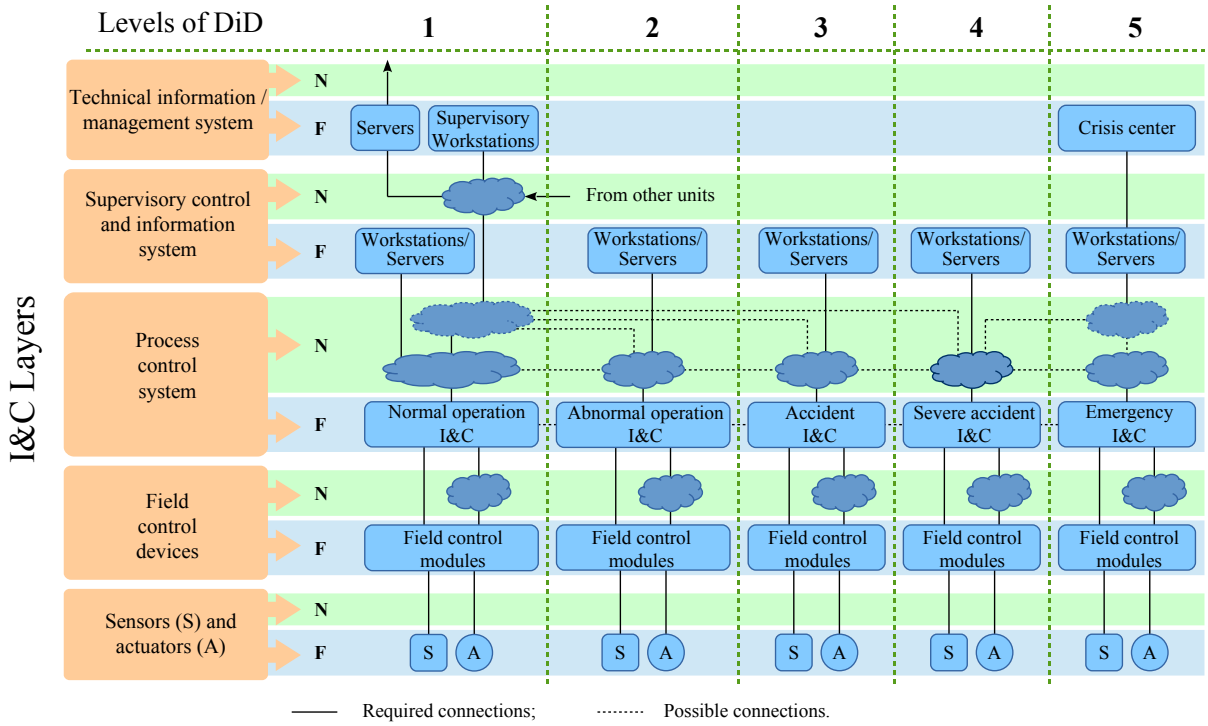



*FIG. 2. Example of a simplified presentation of NPP I&C architectures.*

The first step should specify:

—The nature of the systems to be reviewed (e.g. a complete I&C architecture, particular operational systems, or I&C platforms);

—The precise identification of system components (e.g. names and version numbers);

—A short description of each (sub)system including its main functions;

—The position and roles of each system in the overall I&C architecture, including assignment to a level of defence in depth and to I&C layers;

—Classification of the system according to national classification and the corresponding classification of the IAEA;

—Boundaries, relationships and connections with other systems and equipment;

—The topics to be covered by the review (see Appendix I);

—A glossary of terms with a project specific meaning, or with a meaning different from the IAEA's and international practice.

Table 2 provides an overview of the different classification schemes implemented in different regulatory regimes and consensus standards. In each Member State, there are requirements and conventions that define how the I&C systems in each class should be designed and implemented. The counterpart is requested to relate their national safety classification scheme to the IAEA scheme in the advance information package.

TABLE 2. SAFETY CLASSIFICATION SCHEMES APPLIED TO INSTRUMENTATION AND CONTROL SYSTEMS

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

The first step of AIP may also include any useful background information, such as:

—Why the IERICS mission was requested;

—The development history of the system under review and the roles of the various intervening organisations, including the counterpart;

—If applicable, what system the system under review is replacing and what improvements are expected from the new system;

—Other applications where the system may be applied.

The review team will ask for clarification of the information in the first step. The question and answer phase should be completed within a time period as short as possible. Thus, questions and answers should be precise and focused, and should be limited to the purpose of the first step and not impinge on the second step. Both the IERICS team and the counterpart will need to be as reactive as possible.

*Second step*

The objective of the second step is to provide more detailed information on the design of the systems under review and on development activities, so that each system can be assessed against the specified review topics. Based on the information in the first step, the review team will specify certain information to be provided in the second step.

Depending on the review topics, this may include the description of the defence in depth concept and its application in the systems, data communication between I&C systems belonging to different levels of defence and between I&C systems of different safety classes, possible ways of failure propagation among the systems and protection against it, the application of diversity in the systems, failure modes and effects analysis to confirm that system effects resulting from software failures are covered, the connection to lower safety class systems, including engineering and / or diagnostic workstations.

In addition to this information, the second step should also include (as a minimum):

—An extension of the glossary, covering the terms used in the second step.

—The list of national standards and regulations that have been applied.

—A self-assessment by the counterpart against the recommendations of SSG–39 [1] regarding the selected review topics. This self-assessment presents, for each such recommendation, the basis for why the counterpart thinks each system complies with the recommendation, preferably with a traceability matrix between the recommendations and the design features presented in the second step.

—Any further information necessary for the assessment of the system.

The counterpart should start preparing the advance information package early enough so that the second step of it is submitted to the review team at least three months prior to the review mission.

On the basis of the information provided in the second step, the review team will issue a list of questions to be communicated to the counterpart prior to the review mission and that will be discussed during the mission.

The IERICS team leader should supplement the advance information package with additional resources and administrative information, such as electronic templates for the mission report, issue sheet template and good practice sheet template for the review mission.

### 2.2.7. Code of conduct

The counterpart should have a set of procedures covering the expectations for the code of conduct appropriate to the facilities being visited by the IERICS team. Compliance with these procedures must be adhered to ensure that the review is carried out appropriately. It is the responsibility of the counterpart to provide these procedures as part of the advance information package in order to get the IERICS team members to understand and agree with their content prior to the initial review visit.

The types of procedures likely to apply are as follows:

—Handling of sensitive information;
—Health and safety at the facilities;
—Policies and procedures for working at the facility.

In addition, there may be circumstances where IAEA expectations for code of conduct are applicable. If this is the case, then these too must be discussed and agreed with the IERICS team members before the review mission takes place.

The code of conduct may also include rules or suggestions pertaining to the cultural codes of the counterpart and to the cooperation within the IERICS team.

### 2.2.8. Logistics

The finalization of the logistical support for the review mission should be completed well in advance of the mission. This includes, but may be not limited to:

—Visa support letters for the IERICS team members and IAEA staff, as applicable;
—Accommodation for the IERICS team during the review mission;
—Transportation of the IERICS team members to this accommodation and the counterpart's facilities;
—Meeting and presentation facilities during the review mission, including for the internal meetings of the IERICS team (possibly also at the place of accommodation);
—Availability of necessary counterpart staff and documentation during the technical sessions;
—Contact information that the colleagues and family of IERICS team members can use reach them during the mission;
—Contingency plan and mobile phone contact numbers to be used in the event that any team member encounters delays or other problems during travel and stay.

### 2.2.9. Nondisclosure agreements

Portions of the review material may be deemed as proprietary information and the contents of the mission report itself will be proprietary information. Members of the IERICS team are expected to sign nondisclosure agreements prior to the start of reviewing the advance information package and to manage proprietary information in an appropriate manner.

The counterpart needs to provide reasonable access to proprietary material prior to and during the review process. It is expected that after the closeout meeting, any printed proprietary information provided to the IERICS team is returned to the counterpart (or appropriately disposed of), and any electronic files associated with the review on team members' electronic media is deleted after the draft copy of the mission report has been submitted to the counterpart. Only the IERICS team leader will retain a master copy for future reference.

### 2.2.10. Language barriers

The working language of an IERICS mission is English. Where required, the counterpart is expected to provide translation services during the review mission. In cases where the original design documentation is in a language other than English, a summary of its contents shall be provided to the IERICS team as part of the presentations / discussions. For key documents, the IERICS team may need a translation of the full table of contents and even a translation of selected (or all) portions of the document.

### 2.2.11. Contact with the IERICS team during preparation

To ensure good communications between the IERICS team members, regular contact should be maintained by the IERICS team leader. This will help to minimize the risk that the team is not fully mobilized at the start of the review and avoid the need to instigate contingency plans.

### 2.2.12. Preparatory meeting

The main purpose of the preparatory meeting is to facilitate the preparation of the review mission and to minimize any risks of misunderstanding between the IERICS team leader and the counterpart representative. This is typically a two or three day mission, where the IERICS team leader and possibly some team members meet face to face the counterpart representative and management. The following items should, as a minimum, be discussed and agreed in the preparatory meeting:

—Short summary on the counterpart;
—Counterpart's expectations from the mission;
—Short summary on the IAEA activities in the subject area;
—Summary on the features and conduct of the IERICS missions;
—Experiences with the previous IERICS missions;
—Detailed discussion on the scope and current status of the counterpart's designs, systems and equipment to be reviewed;
—Detailed discussion on the topics of the review (based primarily on SSG–39 [1]);
—Expectations for the AIP;
—Documents to be prepared and used during the main mission;
—Presentations to be prepared by the counterpart for the mission;
—Counterpart's facilities to be visited by the experts;
—Contents of the mission report;
—Target date and time schedule of the mission and the potential follow-up mission;
—Number and list of potential international experts (and potential observers);
—Conditions for the experts (travel, accommodation, per diem, honorarium, etc.);
—Visa arrangement for experts;
—Confidentiality issues;
—Action items to be performed by all parties prior to the mission.

A 'Minutes of the meeting' should be prepared based on the discussions, which should contain the following items:

—Background information;
—Summary of the discussions;
—Preparation of the terms of reference;
—Review basis and reference;
—Review subjects (the system under review);
—Preparation of the advance information package;
—Target date and place for the review, mission duration;

—Names of the IERICS team leader and the counterpart representative;
—Names of the potential review team members;
—Items of agreement;
—Conditions for the experts;
—Action items for all parties prior to the mission.

## 2.3. REVIEW MISSION

### 2.3.1. General guidelines for the review mission

Hereafter are a few general guidelines pertaining to the review mission:

—It is essential for the success of the review to set and maintain a cooperative, professional and courteous atmosphere, both within the IERICS team and between the IERICS team and the counterpart.
—The review mission should be conducted following the review mission agenda. However, flexibility will often be necessary to take into account the findings made during the review (which could require specific investigation) and the contingencies inherent to any activity involving a large number of contributors.
—Throughout the mission, misunderstandings could arise from different interpretations of technical terms, abbreviations and expressions. It is thus necessary for both the IERICS team and the counterpart to maintain a glossary that explicitly defines the terms, abbreviations and expressions that could be misleading.
—Examination of the documents provided by the counterpart must be performed under the procedural requirements of the counterpart. Agreement should be obtained from the counterpart to take documentation away from the facility if required as part of the review. Documentation taken away from the facility should be handled as required by the counterpart.
—Frequent communication between the IERICS team leader and the counterpart representative and management is necessary, e.g. to agree on agenda modifications, to clarify any misunderstandings. In particular, the counterpart representative should have daily meetings with the IERICS team and should be invited to advise the IERICS team when information may not be complete or correct. In cases of misunderstanding or where issues need further clarification, the counterpart representative should be invited to advise the IERICS team of the responsible or knowledgeable counterpart staff in specific areas who can provide clarification to clear the misunderstanding or provide clarification.

### 2.3.2. Briefing meeting

The objective of the briefing meeting is to make sure that the whole IERICS team has all necessary information regarding:

—The objectives, scope and background of the review and the review mission, from the IAEA standpoint; this includes in particular a clear identification of the system under review and of the review basis and reference documents;
—The code of conduct to be applied by the IERICS team members during the review mission;
—The name, background, domains of competence and role of each IERICS team member;

—The review mission agenda;
—The logistics for the review mission, from the IAEA standpoint.

The briefing meeting may also be the opportunity:

—To finalize the initial IERICS questions list resulting from the preparation phase;
—To finalize any pending formalities, such as signing of contracts if necessary;
—To deal with any last minute changes.

Hereafter are a few general suggestions pertaining to the briefing meeting:

—The meeting is typically held the day preceding the review mission per se, and typically lasts for a few hours.
—The briefing meeting is normally chaired by the IERICS team leader.
—As far as practically possible, it should involve all IERICS team members participating in the review mission.
—The IERICS team leader should ensure that each IERICS team member has a copy of terms of reference and is fully aware of its contents prior to the review mission per se.
—In order to ensure that a quasi-final state of the mission report can be reached at the debriefing meeting, the responsibilities within the team for the different sections of the mission report should be allocated and agreed upon during the briefing meeting.
—The counterpart could participate in the meeting as an observer, or to convey information that would be difficult or awkward to address in the plenary opening session.

### 2.3.3. Opening session

The objective of the opening session is to make sure that all the participants to the review mission (IERICS team and counterpart) have all necessary or useful information and understanding regarding:

—The objectives, scope and background of the review and the review mission, from the counterpart and from the IAEA standpoints;
—The counterpart's organization and background;
—The precise identification of the system under review, including its boundaries and environment;
—The review basis and reference;
—The name, background and role of each participant;
—The review mission agenda;
—The logistics for the review mission;
—Any constraints pertaining to confidentiality of information, security and safety of the participants.

The opening session may also be the opportunity for:

—A welcome address and opening remarks by the counterpart;
—A presentation on generic IERICS mission features.

Hereafter are a few general suggestions pertaining to the opening session:

—The meeting is typically held at the very beginning of the review mission per se (excluding the briefing meeting).
—The opening session is normally co-chaired by the IERICS team leader and by the counterpart representative.
—As far as practically possible, it should involve all participants to the review.
—When presenting themselves, the IERICS team members should describe their area of expertise and their experience; this introduction provides the counterpart with a point of reference.
—The counterpart should then be asked to introduce their staff in a similar fashion; IERICS team members should note the members of the counterpart staff who represent their area of interest.
—In the presentation of the system under review, the counterpart should be asked to provide a system overview, showing the overall system architecture, its boundaries and interfaces with its environment and the functional flow of information and control. This overview could allow the counterpart to use presentation materials they may already have.
—The IERICS team members should note areas of interest during the overview, but leave detailed questioning for the technical sessions.

### 2.3.4. Technical sessions

Hereafter are a few general suggestions pertaining to technical sessions:

—The IERICS team and the counterpart should keep the session focused, maintain the session schedule and ensure that discussions remain courteous and cooperative.
—Focus should remain on the objectives of the session, i.e. compliance to the pertaining elements of the review basis and references.
—Upon the end of the session, a discussion with the counterpart should take place in order to clarify any remaining questions from the IERICS team. A list of pending questions that need more time to be answered (i.e. requests for clarification or more information) should be established in written form and agreed upon, and a tentative time table for resolution should be set.
—During the session, the participating IERICS team members should start noting possible issues and good practices.
—In case of a breakout session, the participating IERICS team members should prepare a brief report to inform the other team members.

### 2.3.5. Technical presentations

In a technical presentation, the counterpart has a leading role and presents a specific aspect of the system under review, at a level of detail that allows the IERICS team to assess the system's compliance to the review basis and references. A typical technical presentation has three main phases:

—An introductory phase, where the aspect(s) of the system to be discussed, and the pertaining elements of the review basis and references, are clearly identified;
—A presentation phase, where the counterpart presents the necessary information, in the form either of presentation slides or of documentation items;

—A discussion phase, where the IERICS team asks for clarification or additional details and the counterpart provides immediate answers where possible.

Hereafter are a few general suggestions pertaining to technical presentations:

—Whether interruptions can be made during the presentations should be agreed upon at the beginning of the session by the co-chairs, but interruptions should not prevent the presenters from completing their presentation;
—The presentation slides, if any, should be provided to the IERICS team members in electronic form.

### 2.3.6. Technical visits

Technical visits are usually optional but are very desirable. They may greatly help the IERICS team in obtaining information that would be difficult to gather from the documentation or from technical presentations. They may be performed at various places, such as with the real system on site (where it is operated or to be operated), at a system development facility, at a system testing facility (i.e. a system integration site), at a simulator facility, etc.

Technical visits are usually less structured and their objectives more open than technical presentations and focused reviews, but a few general suggestions may apply:

—Technical visits are usually proposed by the counterpart, but the IERICS team leader may make suggestions, based on the objectives and scope of the review.
—A technical visit usually begins with a short presentation by the counterpart of what is to be seen, of what specific rules and constraints may apply, of the accompanying counterpart staff and their domains of competence, in case IERICS team members have specific questions during the visit.
—The participating IERICS team members may decide, prior to the visit or at the end of the counterpart's presentation, to distribute among themselves the different aspects to be examined during the visit.
—'Surprising' observations during the visit should be shared between the participating IERICS team members, so that possible implications may be assessed more thoroughly.

### 2.3.7. Focused reviews

A focused review follows a specific subject through the counterpart's documentation or presentation to a more detailed level of evaluation and assessment. The issues that are the object of a focused review are usually selected because of their importance with respect to the objectives of the IERICS review, or because they are representative of large parts of the system.

An example of the first category would investigate measures to cope with common cause failures. An example of the second category would follow a particular system function from inputs to outputs through all system layers. Another example of the second category would follow how failures are reported and analysed, and would track a few specific failure events from initial detection to final resolution. In the first and second examples, the focused review follows a purely technical path, whereas in the third example, it follows a work process, evaluating technical aspects at discrete locations.

A focused review is usually under the leadership of the IERICS review team. It is usually composed of three main phases:

—A short definition phase, where the IERICS team explain the subject of, and their objectives for, the review session;
—A short presentation phase, where the counterpart explains how the subject is handled in the system under review or in their work processes and the organization of their pertaining documentation;
—A 'thread analysis' phase consisting in interviews and examination of specific documents or parts of documents by the IERICS team.

Hereafter are a few general suggestions pertaining to focused reviews:

—The list of focused reviews and their scopes are usually determined by the IERICS team leader and are agreed upon by the counterpart. Though it is preferable to plan them ahead of the review mission, some may be decided during the mission based on the questions raised. Enough preparation time should be given to the counterpart so that they may make adequate provisions regarding competent staff and access to documentation.
—IERICS team members should dig deep enough to get a clear understanding of the subject, but they should also guard against wasting time on technical details that are not relevant.

### 2.3.8. IERICS team meetings

These meetings involve only the IERICS team members. The objective of the meetings is to allow the team members to share information and understanding, to compare points of view, to maintain a list of questions and clarification items and to reach a team consensus on findings. Another essential objective is to develop the mission report.

Hereafter are a few general suggestions pertaining to meetings:

—The IERICS team should hold one such session at the end of each day, when impressions and information are still fresh in their minds.
—Meetings are particularly necessary in the case of breakout sessions, so that the whole team may share information.
—During the first few days, meetings will usually tend to be short (typically one hour or less), but as the review mission nears the closeout session, more time is usually necessary to merge the findings of individual team members into a consistent and well organized list.
—Progress regarding the mission report should be checked at each meeting. In order to ensure that a quasi-final state of the report can be reached at the debriefing meeting, any relevant information should be inserted in the report as soon as it is available.
—The IERICS team leader plays an important role in maintaining the cohesion and the focus of the team during meetings.

### 2.3.9. Closeout session

The objectives of the closeout session are:

- For the IERICS team to present their findings (comments, issues, recommendations, suggestions and good practices) to the counterpart;
- For the counterpart to provide their feedback on the IERICS team findings;
- For the IERICS team to make any appropriate adjustments to their findings, or to the way the findings are to be presented in the report.

The closeout meeting is also the opportunity to take leave from the counterpart staff and consider any follow-up action.

Hereafter are a few general suggestions pertaining to the closeout meeting:

- The session is typically held at the very end of the review mission per se (excluding the debriefing meeting).
- The closeout session is normally co-chaired by the IERICS team leader and by the counterpart representative.
- As far as practically possible, it should involve all participants to the review.
- A written list of findings should be provided to the counterpart prior to the session (typically the day before), so that the counterpart has time to prepare their feedback.
- Any adjustment from the written findings should be made clear during the session, in such a way that the counterpart is not 'surprised' by the final findings.

### 2.3.10. Debriefing meeting

The debriefing meeting involves only the IERICS team. Its objective is to develop a quasi-final state for the mission report and to allocate any remaining work within the team.

Hereafter are a few general suggestions pertaining to the debriefing meeting:

- The meeting is typically held the day following the review mission per se, and typically lasts a few hours.
- The meeting is chaired by the IERICS team leader.
- As far as practically possible, it should involve all IERICS team members participating in the review mission.
- The responsibilities within the team for the finalization of the mission report should be allocated and agreed upon during the debriefing meeting.

## 2.4. FOLLOW-UP MISSION

The objective of a follow-up mission is to assess progress made in the resolution of the issues identified and in particular in the implementation of the recommendations and possibly of the suggestions. Hence, a follow-up mission should in principle be requested only when the resolution of issues has reached a sufficient level of maturity. In particular, a follow-up mission is most appropriate when in the counterpart's view the action is completed.

The counterpart may elect to request a follow-up mission even when the actions are not fully completed, but planned only. The goal of this mission is to assess the plan and to provide technical advice on any of the action items. In this case a final follow-up mission may be necessary to close the issues.

A subsequent follow-up mission may also be requested by the counterpart to resolve any pending issues that remained open in a previous follow-up mission.

General guidelines:

—Decision, scope and timing are based on a mutual agreement between the IERICS team leader and the counterpart.

—The follow-up mission team should be composed of the team leader and preferably two or three other members of the original review team.

—It should be performed typically 12 to 18 months after the main mission.

—It should last typically for three days, depending on the volume and complexity of work.

—There should be a preparation phase like for the main review mission. The counterpart sends in advance to the IAEA all issue sheets from the main mission, having completed the recent status of issues and the response to recommendations / suggestions. The form of it may be a one-step advance information package similar to what has been provided prior to the main mission.

—The guidelines for the main review mission also apply.

## 2.5. REPORTING AND DOCUMENTING

### 2.5.1. Mission report

The mission report is the deliverable of the IERICS team for the mission. It presents the background, objective and scope of the mission, the system under review, the review basis and reference, and the findings made by the team during the review. A suggested report format is provided in Appendix II of this publication.

Findings may be classified into two categories: (1) issues, and (2) good practices, and are discussed in more details in the following sections. Figure 3 provides an overview of how the mission findings will be resolved and documented in the mission report.

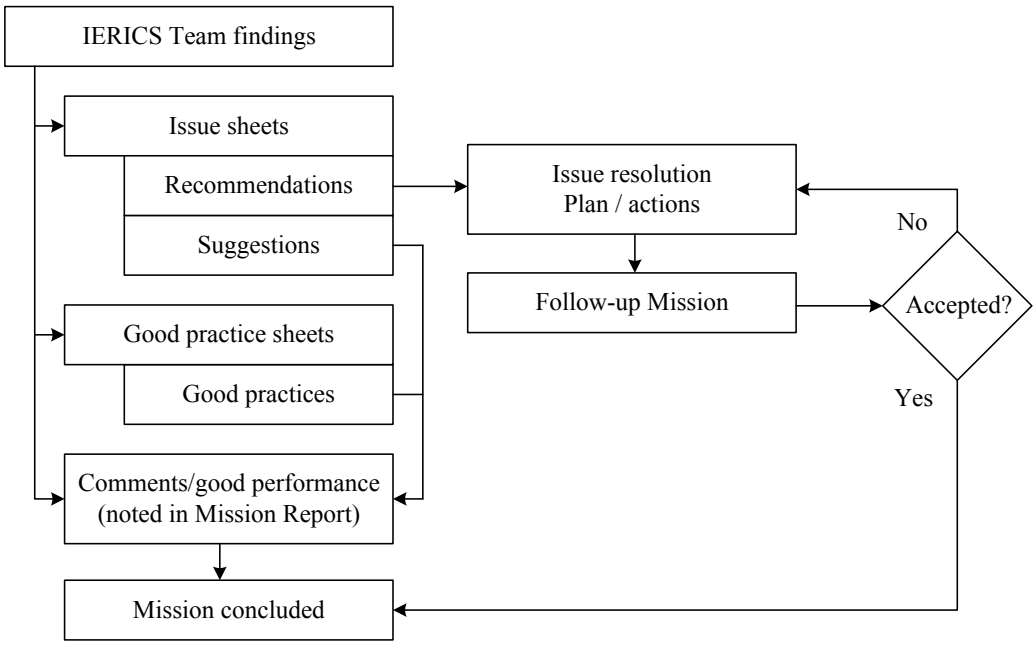



*FIG. 3. Resolution of the mission findings.*

### 2.5.2. Issues and issue sheets

An issue is an identified concern or an area of improvement, which has been identified on the basis of the review basis and reference and/or the internationally recognized good practices in the topic. Each issue is presented in an issue sheet, which addresses the following topics:

(1) Issue identification, with issue number and title, mission name, reviewed area.
(2) Issue clarification, with issue description, issue origin (IAEA review team or counterpart), source documents and reference to any other relevant documents.
(3) Counterpart's view on the issue.
(4) Assessment by the IERICS team, with comments, recommendations and suggestions.
(5) Counterpart's response on recommendations and suggestions.
(6) Counterpart's actions taken after the mission and prior to the follow-up assessment.
(7) Follow-up assessment by the IERICS team, with possibly new comments, recommendations and suggestions.
(8) Status of the issue (no action, actions planned or under way, issue partially resolved, issue completely resolved).

An issue sheet template is given in Appendix III of the mission report.

**Sections 3, 5 and 6**

The purposes of Sections 3, 5 and 6 of the issue sheets are to reflect the views of and the measures taken by the counterpart for the issue resolution. They are optional and the counterpart may choose not to fill them in.

**Sections 4 and 7**

The purposes of Sections 4 and 7 of the issue sheets are to reflect the discussions with the counterpart experts, to record the conclusions, to issue possible recommendations and suggestions and to synthesize the IERICS team judgment on the resolution of the issue under discussion. However, the IERICS team should not be too prescriptive in the methods to resolve the issue, and suggest only the goals to be reached. However, advice can be given if requested.

**Subsections 4.1 and 7.1 - Comments**

They are observations of the IERICS team based on the review and the discussions during the mission. It is for information only, no action or response is required from the counterpart.

**Subsections 4.2 and 7.2 - Recommendations and suggestions**

A recommendation is advice from the IERICS team on what improvements should be made that would contribute to resolve an issue. Follow-up actions are required for recommendations. A recommendation is usually made when the guidance of SSG–39 [1] is not met.

A suggestion is also advice from the IERICS team on what improvements may be made that would contribute to resolve an issue. Follow-up actions are optional for suggestions, as suggestions are primarily made to bring design and/or procedures more in line with internationally recognized good practices.

If an item is not considered significant enough to meet the criteria of a suggestion, but the IERICS team feels that mentioning it is still considered significant, a comment regarding the item may be made in the text of the mission report (e.g. "the team encouraged the operating organization to…").

Recommendations, suggestions and comments, are numbered in sequential order for further reference. The reviewed documents (corresponding specifically to the issue under consideration) are also listed.

As much as possible, each recommendation and suggestion should be referenced to the relevant requirement/recommendation of respective review basis and reference documents.

**Status of the issue**

The status of the issue under consideration is assessed during the follow-up mission and the respective resolution degree is assigned to reflect the judgment of the IAEA review team. The degree is scaled from 1 to 4, as indicated in the issue sheet template.

For the resolution of some recommendations, additional follow-up actions may be agreed upon to clarify not only plans but also actions to implement these plans. Either party may recommend performing additional assessment to verify the implementation of the plans after an agreed upon completion deadline. In this case a subsequent follow-up mission should be organized (see also Section 2.4 and Fig. 3.).

### 2.5.3. Good practices and good practice sheets

A good practice is an outstanding and proven performance, programme, activity or design element in use that contributes directly or indirectly to system safety and sustained good performance. A good practice is markedly superior to other practices observed elsewhere, not just in its fulfilment of current requirements or expectations. It should be sufficiently superior and have broad enough application to be brought to the attention of other NPPs, suppliers, assessors, integrators, etc., and be worthy of their consideration in the general drive for excellence. A good practice has the following characteristics:

—It is novel;
—It has a proven benefit;
—It can be used at other plants;
—It does not contradict an issue.

The attributes of a given good practice (e.g. whether it is well implemented, or creative, or it has good results) should be explicitly stated in the description section of the good practice sheet.

Note: An item may not meet all the criteria of a good practice, but still be worthy to take note of. In this case it may be referred to as 'good performance' and may be documented in the text of the report. A good performance is a superior objective that has been achieved or a good technique or programme that contributes directly or indirectly to system safety and sustained good performance that works well at the plant. However, it might not be necessary to recommend its adoption by other NPPs, because of financial considerations, differences in design or other reasons.

A good practice sheet template is given in Appendix IV of the mission report.

### 2.5.4. Notification of mission completion

Upon the successful completion of the review and mutual concurrence on the content of the mission report, the IAEA will send the report to the counterpart through official governmental channels.

The letter from the IAEA will shortly summarize the subject of the review, the review criteria assessed, successful mission completion, etc. A suggested version of the IAEA notification letter text can be seen below. Text in italics should be replaced with the attributes of the given IERICS mission.

"Excellency *or Sir or Madam*,

I have the honour to inform you that the International Atomic Energy Agency's (IAEA's) Independent Engineering Review of Instrumentation and Control Systems (IERICS) mission and its follow-up mission on the *'Name of the reviewed system'*, which were carried out *'from – to date and location of the main and follow-up mission'*, respectively, have been completed successfully. The Safety Guide *Design of Instrumentation and Control Systems for Nuclear Power Plants* (IAEA Safety Standards Series No. SSG–39) and other related IAEA nuclear safety and nuclear energy publications formed the basis of criteria for this review.

Please find attached the final mission report, which identifies *number (99)* recommendations, *number (99)* suggestions and *number (99)* good practices. The Executive Summary includes the final conclusions of the IERICS mission.

In its entirety, the enclosed final mission report is restricted and no copies will be distributed, unless a request for derestriction is received from your office. With your concurrence, the IAEA may share the good practices with other stakeholders in the nuclear power I&C industry.

Accept, Excellency *or Sir or Madam*, the assurances of my highest consideration."

### 2.5.5. Use of the mission report

With the concurrence of the counterpart, the 'Executive summary' of the final mission report will be posted on the IERICS mission page of the IAEA public website. This post will include the contact information of the assigned person at the counterpart, should interested stakeholders from the Member States want to communicate with the counterpart for further information exchange. Additionally, the good practices identified during the mission will be specifically listed along with the 'Executive summary'. The objective of identifying good practices is to have them be brought to the attention of other NPPs, suppliers, assessors, integrators, etc. The counterpart should inform the IAEA scientific secretary whether only the titles of good practices, or the full good practice sheets (without editing) may be posted on the IAEA webpage.

In its original form, the final mission report is confidential. However, the counterpart may elect to share the entire report with selected organizations or individuals. The counterpart can also refer to the successfully completed IERICS mission and its final mission report in their presentations, brochures, leaflets, etc. However, the counterpart may not make any edits, deletions, or reorganization of it. Also, the report shall not be considered and shall not be referred to as a 'product certificate', a 'regulatory inspection', or an 'audit made by the IAEA against national or international codes and standards', but rather as the summary of a technical peer review.

# 3. REVIEW PRINCIPLES

The IERICS mission is intended to conduct reviews of I&C system design documentation, prototype systems and systems in actual operation at the plant. The IERICS mission is based on appropriate IAEA publications, such as Safety Guides and Nuclear Energy Series publications.

The Safety Guides, specifically SSG–39 [1], should be used to establish the review basis. Typically, the following sections from SSG–39 may be addressed as part of the review:

—The management system for I&C design;
—Design basis for I&C systems;
—I&C architecture;
—Safety classification of I&C functions, systems and equipment;
—General recommendations for all I&C systems important to safety;
—Design guidelines for specific I&C systems and equipment;
—Considerations relating to the human-machine interface;
—Software.

From these sections, specific requirements for the mission can be drawn. Appendix I gives more details on potential review topics.

Obtaining information during the review should be based on observations, interviews, document reviews and facility / equipment walk downs. Information obtained through the above process becomes an important foundation for the overall review results.

## 3.1. REVIEW TECHNIQUES

The IERICS review team uses five steps to acquire the information needed to develop their recommendations/suggestions. The five steps are:

(1) Review of written material and / or presentations;
(2) Discussion and interviews;
(3) Direct observation of programme implementation and the status of the I&C systems;
(4) Discussions among the review team;
(5) Discussion of evaluations/tentative conclusions with counterparts.

### 3.1.1. Use of review techniques

The use of review techniques mentioned above should be planned in advance. Arrangements should be made with the counterpart as to how to perform the discussions / interviews and observations.

The IAEA review team has meetings, in which the experts present their actual findings, summarize their concerns developed during the reviews and discuss actual issues. This creates an opportunity for other team members to contribute their views, further strengthening the experience base of the evaluation. It is important that each expert comes to the meeting prepared to make a concise statement of their findings, in order to allow the other review areas to be discussed at the same meeting. These meetings will determine those issues to be presented to the counterpart for consideration by the counterpart's organization. A template for the issue sheets is shown in Appendix III of the mission report.

Formulation of comments, recommendations and suggestions should be based on the identified issues. Similarly, good practices discovered during the process of the review that

should be documented for the benefit of other Member States are described in the good practice sheets in sufficient detail as to be readily understood.

Based upon the discussions and observations, the reviewers can, if necessary, modify their preliminary view. Multiple cycles of document review, discussions, interviews and observations may be required for the clarification and resolution of complex issues and/or findings.

### 3.1.2. Review of written material

Appendix I of this publication provides a broad range of I&C topics and issues that the IERICS team may consider for further discussion during the IERICS review. The scope of the review mission will dictate which portions of the appendix are relevant (within the scope of the review mission).

Reviewers should consider and utilize this material during their review of the advance information package in both the preparatory phase and the implementation phase of the IERICS mission.

### 3.1.3. Presentations, discussion and interviews

The IERICS team will conduct discussions / interviews with the counterpart to:

—Provide additional information not covered by the advance information package;

—Answer questions and satisfy concerns arising out of the documentation review;

—Obtain an in-depth understanding of:

- The important characteristics of the system;
- The development processes applied (lifecycle, V&V, methods, ...);
- The associated work procedures and activities.

—Form a joint judgment on the findings.

The discussions / interviews are also used to provide the opportunity for exchanging all the important information between the IERICS team members and their counterparts, and therefore should be held at the working level between peers. These interviews should be a ‘give and take’ discussion and not an interrogation of the counterparts by the team members. Properly conducted, these discussions / interviews are possibly the most important part of the IERICS mission.

In addition, presentations by the counterparts (both formal and informal) can be used as a means of obtaining further information and to fill in the information gaps identified as a result of the review of the advance information package.

Where possible, equipment demonstrations and technical visits may be held to provide the review team with a deeper understanding of the system. This may include demonstrations with prototype hardware/systems or at system test and validation facilities.

### 3.1.4. Direct observation of performance, status and activities

Direct observation of the application of processes and use of procedures supporting the design, functionality, testing, operation and performance of the system under review means onsite observation of the following:

—Implementation of development procedures and plant programmes:

- Use of procedures, tools and instructions;
- Regular and specific reporting;

- Quality assurance and quality control processes;
- Collection, storage and retrieval of data;
- Configuration management;
- Change control;
- Record keeping and trend monitoring;
- Arrangement for monitoring of effectiveness of the processes;
- Management control.

—Where appropriate, physical conditions of the selected I&C systems within the scope of the review:
- Equipment walk-downs;
- Inspection reports.

From these observations, the reviewers will form a position on:

—The quality of the processes supporting the design, functionality, testing, operation and performance;
—The level of commitment of the staff and the overall safety culture of the counterpart;
—Capability of the staff in terms of resources and technical knowledge and skills;
—The overall condition of the facilities and I&C systems within the scope of the review.

## 3.2. INFORMATION PROVIDED BY THE COUNTERPART

Examples of the main information sources to be provided by the counterpart are as follows:

—The advance information package;
—Design basis documentation:
- System and equipment specifications;
- Design documents;
- Test reports;
- Qualification reports;
- Reliability evaluation reports;
- V&V documentation;
- Configuration management procedures.

—Programme for modifications and replacements, rationales for previous modifications (based on operations feedback where applicable);
—Lifecycle management and processes;
—Already identified issues and good practices based on a self-assessment by the counterpart.

The scope of information sources should be defined and agreed in the terms of reference.

## 3.3. DEVELOPMENT OF THE MISSION FINDINGS

During the course of the review, the IERICS team will hold internal consolidation sessions (IERICS team meetings) to develop a common set of findings. The team will write down the issue and good practice sheets and will update them as necessary after discussion with the counterpart. In writing the sheets, the following should be taken into account:

—Emphasis should be given to the reviewers' observations with minimum description and clear conclusions.
—Wherever possible, reference to IAEA safety standards and other reference documents should be provided.
—Language should be clear, concise, objective and impersonal.
—Short, direct sentences aid understanding.
—Official names should be used to designate organizational units, positions and systems.
—Abbreviations or acronyms shall be introduced upon their first use and compiled in a list.

The issue and good practice sheets should be written in English and modified and supplemented, if necessary, through the entire period of the review. Templates for the issue sheet and good practice sheet are provided in the mission report template in Appendix II of this publication.

## 3.4. WORKING WITH THE COUNTERPART

Besides the interviews and meetings with the counterpart described in Section 3.1, the work with the counterpart on site involve the following activities:

—The opening session;
—Regular meetings arrangements (meeting with the counterpart, summary team meetings, etc.);
—The closeout session.

During the opening session with the counterpart, the organization and performance of the review should be presented. Possible, focused working teams for specific areas may be established. The working teams in each area consist of designated IERICS team members, counterpart experts and their technical support. It is advisable to daily have a short regular meeting of all participants to discuss the actual organizational issues for the working day.

The mission's schedule might be adjusted on a daily basis during the course of the mission to ensure that sufficient progress is achieved. Any changes should be discussed and agreed with the counterpart.

The counterpart should be informed on a regular basis of the preliminary findings and recommendations made by the review team. Whenever possible, an agreement should be reached between the IERICS team and counterpart on every finding and recommendation. Representatives of the counterpart may attend the daily team meeting upon invitation.

The day before the closeout session, the IERICS team experts should deliver their part of the mission report as already agreed upon with the counterpart.

A formal closeout session is held the last day of the review mission. At this session, all the IERICS team members provide short conclusive statements summarizing findings, recommendations and suggestions.

# REFERENCES


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

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

[3] 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).

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

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementing Digital I&C Systems in the Modernization of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-1.4, IAEA, Vienna (2009).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Protecting Against Common-Cause Failures in Digital I&C Systems, IAEA Nuclear Energy Series No. NP-T-1.5, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Integration of Analog and Digital Instrumentation and Control Systems in Hybrid Control Rooms, IAEA Nuclear Energy Series No. NP-T-3.10, IAEA, Vienna (2010).

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

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

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

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.17, IAEA, Vienna (2016).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance, IAEA-TECDOC-1402, IAEA, Vienna (2004).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Managing Modernization of Nuclear Power Plant Instrumentation and Control Systems, IAEA-TECDOC-1389, IAEA, Vienna (2004).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Solutions for Cost Effective Assessment of Software Based Instrumentation and Control Systems in Nuclear Power Plants, IAEA-TECDOC-1328, IAEA, Vienna (2003).

# APPENDIX I

# TOPICS FOR THE IERICS MISSION

The objective of this appendix is to help the IERICS team leader and the counterpart clarify the scope and the basis of the IERICS mission. It suggests a list of topics that could be considered and discussed. The list of topics may also be used by the IERICS team leader and the counterpart to determine the technical sessions to be included in the IERICS mission agenda.

The IERICS team leader and the counterpart should feel free to include in their discussion any other topic that might be relevant to the mission.

The proposed topics are organized into 10 main themes:

(1) System identification;
(2) The management system for I&C design;
(3) Design basis for I&C systems;
(4) I&C architecture;
(5) Safety classification of I&C functions, systems and equipment;
(6) General recommendations for all I&C systems important to safety;
(7) Design guidelines for specific I&C systems and equipment;
(8) Considerations relating to the human-machine interface;
(9) Software;
(10) Operation & maintenance processes review.

For each theme, a table in this appendix lists the associated topics. The tables have four columns:

—The ‘ID’ column associates a code to each topic for further reference.
—The ‘Topic and description’ column explains what the topic is about.
—The ‘SSG–39 clauses’ column provides the references to relevant recommendations in the IAEA safety guide.
—The ‘Remark’ column provides additional information to facilitate understanding of the topic.

This appendix is available in editable electronic form. The IERICS team leader and the counterpart would typically:

—Select the topics relevant to the given mission during the preparatory phase. It will provide guidance to the counterpart on what information to include in the AIP.
—Add new lines for any topics that need to be addressed and were not in the tables.

## 1. SYSTEM IDENTIFICATION

The objective of system identification is to provide general information regarding the system that will serve as background information when addressing the other themes. The topics listed here are the basis for and should be covered in the first step of the AIP.

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| ID1 | **System identification**<br>Unambiguous identification of the system to be reviewed, including name and version. | 2.38, 2.42, 2.50 | |
| ID2 | **System description**<br>Main functional objectives, main characteristics of the system. | 2.1, 2.90 (bullets 2, 4, 5), 3.2, 3.6, 4.12 | |
| ID3 | **The position and roles of the system in the overall I&C architecture**<br>Roles of the system, assignment to a level of defence in depth and to I&C layers. | 4.1, 4.6, 4.13, 4.28 | |
| ID4 | **System composition**<br>Identification and description of the main subsystems / components of the system, identification of their versions. | 2.90 (bullets 6, 7), 2.96, 4.2, 4.13 | |
| ID5 | **Classification of the system and components** | 5.1 to 5.13 | See SC1. |
| ID6 | **System boundaries and interfaces**<br>Limits of the system, identification of the entities interacting with the system (equipment, other systems, personnel), characteristics of interfaces. | 2.90 (bullet 8), 2.96 (bullet 4), 4.2, 4.11 | |
| ID7 | **Application(s) of the system**<br>Intended uses of the system, where applicable. | 2.90 (bullet 4), 3.10, 3.15, 4.1, 4.11, 4.13, 5.2 | |
| ID8 | **System physical environment**<br>Characteristics of the physical environment of the system, including ambient conditions, seismic conditions, etc. | 3.14 (main bullet 4), 6.96, 6.97, 6.108, 6.113, 6.114 | |
| ID9 | **System development history**<br>Overview of the different stages that led to the current version of the system. Identification of the different organizations that were implied during this history and their roles and responsibilities. | 2 (2.2, 2.6, 2.7, 2.17, 2.20, 2.22, 2.23) | |

## 2. THE MANAGEMENT SYSTEM FOR I&C DESIGN

The term *management system* has been adopted in the revised standards instead of the terms *quality assurance* and *quality assurance* programme. The objective of the system review is to assess compliance with the recommendations of Section 2 "*The management system for I&C design"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| MS1 | **Management system**<br>A set of interrelated or interacting elements (systems) for establishing policies and objectives and enabling the objectives to be achieved in an efficient and effective manner.<br>• The component parts of the *management system* include the organizational structure, resources and organizational *processes*. Management is defined (in ISO 9000) as coordinated *activities* to direct and *control* an organization.<br>• The *management system* integrates all elements of an organization into one coherent system to enable all of the organization's objectives to be achieved. These elements include the organizational structure, resources and *processes*. Personnel, equipment and organizational culture as well as the documented policies and *processes* are parts of the *management system*. The organization's *processes* have to address the totality of the *requirements* on the organization as established in, for example, IAEA *safety standards* and other international codes and standards. | 2.1 to 2.9 | |
| MS2 | **Life cycle models**<br>Representations of the development processes that describe the activities for the development of systems and the relationships between these activities. | 2.10 to 2.23 | |
| MS3 | **Process planning**<br>Identification of the necessary inputs and the products and processes of an activity, and the relationship of the activity with other activities. | 2.24 to 2.28 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| MS4 | **Coordination with human factors engineering activities and computer security activities**<br>• Human factors engineering: Engineering in which factors that could influence human performance are taken into account.<br>• Information security: The preservation of the confidentiality, integrity and availability of information. Note: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.<br>• Computer security: A particular aspect of information security that is concerned with computer based systems, networks and digital systems. | 2.29 to 2.37 | |
| | **Activities common to all life cycle phases** | | |
| MS5 | **Configuration management**<br>The *process* of identifying and documenting the characteristics of a *facility*'s *structures, systems and components* (including computer *systems* and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the *facility* documentation. | 2.38 to 2.55 | 'Configuration' is used in the sense of the physical, functional and operational characteristics of the *structures, systems and components* and parts of a *facility*. |
| MS6 | **I&C systems hazard analysis**<br>Process of examining a system throughout its lifecycle to identify inherent hazards and contributory hazards and requirements and constraints to eliminate, prevent, or control them. | 2.56 to 2.65 | The scope of hazard analysis extends beyond design basis accidents for the plant by including abnormal events and plant operations with degraded equipment and plant systems. |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| MS7 | **Verification**<br>The *process* of determining whether the quality or performance of a product or service is as stated, as intended or as required.<br>**Computer system verification**<br>The *process* of ensuring that a phase in the *system* life cycle meets the requirements imposed on it by the previous phase.<br>**Validation**<br>The *process* of determining whether a product or service is adequate to perform its intended function satisfactorily.<br>**Computer system validation**<br>The *process* of testing and evaluating the integrated computer *system* (hardware and software) to ensure compliance with the functional, performance and interface requirements. | 2.66 to 2.74 | *Verification* is closely related to *quality assurance* and *quality control*.<br>*Validation* is broader in scope, and may involve a greater element of judgement, than *verification.* |
| MS8 | **Use of insights from probabilistic safety analysis**<br>A comprehensive, structured approach to identifying *failure scenarios*, constituting a conceptual and mathematical tool for deriving numerical estimates of *risk*. | 2.75 to 2.77 | |
| MS9 | **Safety assessment**<br>1. *Assessment* of all aspects of a *practice* that are relevant to *protection and safety*; for an *authorized facility*; this includes *siting*, *design* and *operation* of the *facility*.<br>2. *Analysis* to predict the performance of an overall *system* and its impact, where the performance measure is the radiological impact or some other global measure of the impact on *safety*.<br>3. The systematic *process* that is carried out throughout the *design process* to ensure that all the relevant *safety requirements* are met by the proposed (or actual) *design*. *Safety assessment* includes, but is not limited to, the formal *safety analysis*. | 2.78 to 2.87 | |
| MS10 | **Documentation** | 2.88 to 2.91 | |
| | **Life cycle activities** | | |
| MS11 | **Requirements specification**<br>Statement of all what the system is required to satisfy. | 2.92 to 2.107 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| MS12 | **Selection of predeveloped items**<br>Item that already exists, is available as a commercial or proprietary product, and is being considered for use in an I&C system. Pre-developed items include hardware devices, pre-developed software, commercial off the shelf devices, digital devices composed of both hardware and software, or hardware devices configured with hardware definition language or predeveloped blocks. | 2.108 to 2.117 | |
| MS13 | **System design and implementation** | 2.118 to 2.123 | |
| MS14 | **System integration**<br>Phase of the system life cycle where the system components, subassemblies and subsystems are progressively assembled together to verify that they operate as designed in the integrated system to enable the system to meet its specified requirements. | 2.124 to 2.127 | |
| MS15 | **System validation** | 2.128 to 2.142 | |
| | **Installation, overall I&C integration and commissioning** | | |
| MS16 | **Installation**<br>of the I&C system on site. | 2.143 to 2.151 | |
| MS17 | **Overall I&C integration**<br>Testing of interconnected systems to confirm that all interfaces of interconnected systems operate correctly, and that failure detection, corrective actions and the display of associated data are operating in accordance with the requirements specification of the I&C functions. | 2.143 to 2.151 | |
| MS18 | **Commissioning**<br>The *process* by means of which *systems* and *components* of *facilities and activities*, having been constructed are made operational and verified to be in accordance with the *design* and to have met the *required* performance criteria. | 2.143 to 2.151 | |
| MS19 | **Operation and maintenance** | 2.152 to 2.156 | |
| MS20 | **Modifications** | 2.157 to 2.167 | |

## 3. DESIGN BASIS FOR I&C SYSTEMS

The objective of the system review is to assess compliance with the recommendations of Section 3 "*Design basis for I&C systems"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| DB1 | **Identification of I&C functions**<br>Functions (and corresponding non-functional requirements for properties such as safety, security and timing constraints) required of the I&C systems. | 3.1 to 3.6 | |
| DB1 | **Content of design basis for I&C systems**<br>Specification of the necessary capability, reliability and functionality of items important to safety for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant. | 3.7 to 3.16 | |

## 4. I&C ARCHITECTURE

The objective of the system review is to assess compliance with the recommendations of Section 4 "*I&C architecture"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| AR1 | **Architectural design** | 4.1 to 4.10 | |
| AR2 | **Content of the overall I&C architecture**<br>The architectural design for the overall I&C establishes:<br>• The I&C systems that comprise the overall architecture;<br>• The organization of these systems;<br>• The allocation of I&C functions to these systems;<br>• The interconnections across the I&C systems and the respective interactions allocated and prohibited;<br>• The design constraints (including prohibited interactions and behaviours) allocated to the overall architecture;<br>• The definition of the boundaries among the various I&C systems. | 4.11, 4.12 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| AR3 | **Content of individual I&C system architectures**<br>The architectural design for individual I&C systems establishes:<br>• The composition – decomposition relationships through all levels of integration down to the indivisible, individual item;<br>• The allocation of I&C functions, behaviours, constraints and (derived) quality requirements to each item at each level of integration;<br>• Rules of composability and composition to provide assurance that the composition of behaviours at one level of integration satisfies the behaviours required at the next, higher level of integration and does not introduce other behaviours;<br>• The interconnections across items at each level of integration and across levels of integration and the respective interactions allocated and prohibited;<br>• The design constraints (including prohibited interactions and behaviours) allocated to each individual I&C system. | 4.13 | |
| AR4 | **Independence** (at architectural design level)<br>Independent equipment possesses both of the following characteristics:<br>• The ability to perform its required function is unaffected by the operation or failure of other equipment;<br>• The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function. | 4.14 to 4.24 | Independence may be obtained by use of the following features:<br>• Physical separation.<br>• Electrical isolation.<br>• Functional independence.<br>• Independence from the effects of communications errors.<br>See also GR5. |
| AR5 | **Consideration of common cause failure**<br>Common cause failure – failure of two or more structures, systems and components in the same manner or mode due to a single event or cause. | 4.25 to 4.40 | See also GR6. |

## 5. SAFETY CLASSIFICATION OF I&C FUNCTIONS, SYSTEMS AND EQUIPMENT

The objective of the system review is to assess compliance with the recommendations of Section 5 "*Safety classification"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SC1 | **Safety classification of I&C functions, systems and equipment**<br>All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance. | 5.1 to 5.13 | See also Table 2. |

## 6. GENERAL RECOMMENDATIONS FOR ALL I&C SYSTEMS IMPORTANT TO SAFETY

The objective of the system review is to assess compliance with the recommendations of Section 6 "*General recommendations for all I&C systems important to safety"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| GR1 | **Unnecessary complexity avoidance**<br>The intent of avoiding complexity is to keep the I&C system as simple as possible but still fully meet its safety requirements. | 6.1 to 6.5 | |
| GR2 | **Reliability**<br>The probability that a system or component will meet its minimum performance requirements when called upon to do so. | 6.6 to 6.9 | |
| GR3 | **Single failure criterion**<br>A criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure. | 6.10 to 6.19 | |
| GR4 | **Redundancy**<br>Provision of alternative (identical or diverse) structures, systems and components, so that anyone can perform the required function regardless of the state of operation or failure of any other. | 6.20, 6.21 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| GR5 | **Independence**<br>The objective of independence is the prevention of failure propagation, by use of the following features: physical separation, electrical isolation, functional independence, independence from the effects of communications errors. | 6.22 to 6.56 | See also AR4. |
| GR6 | **Diversity**<br>The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure. | 6.57 to 6.63 | See also AR5. |
| GR7 | **Failure modes**<br>The manner or state in which a structure, system or component fails. | 6.64 to 6.76 | The concept of failsafe design shall be incorporated, as appropriate, into the design of systems and components important to safety (SSR 2/1). |
| GR8 | **Equipment qualification**<br>Generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements. | 6.77 to 6.90 | |
| GR9 | **Suitability and correctness** (during equipment qualification)<br>Part of the qualification process that verifies that the equipment is appropriate for the intended function. | 6.91 to 6.95 | |
| GR10 | **Environmental qualification**<br>Environmental qualification is qualification for temperature, pressure, humidity, chemical exposure, radiation, submergence, electromagnetic phenomena and ageing mechanisms that affect the proper functioning of components under those conditions. | 6.96 to 6.107 | |
| GR11 | **Internal and external hazards**<br>Safety analyses will identify internal and external hazards, such as fire, flooding and seismic events, which the plant is required to tolerate for operation or which the plant is required to withstand safely. | 6.108 to 6.112 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| GR12 | **Electromagnetic qualification**<br>Electromagnetic compatibility is the ability of a system or component to function satisfactorily in its electromagnetic environment without the introduction of intolerable electromagnetic disturbances to anything in that environment. | 6.113 to 6.134 | |
| GR13 | **Design to cope with ageing and obsolescence**<br>Ageing is a general process in which characteristics of a structure, system or component gradually change with time or use.<br>Physical ageing happens due to physical, chemical and/or biological processes (ageing mechanisms).<br>Non-physical ageing (obsolescence) is the process of becoming out of date (i.e. obsolete) owing to the evolution of knowledge and technology and associated changes in codes and standards. | 6.135 to 6.152 | |
| GR14 | **Control of access to systems important to safety**<br>Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented. | 6.153 to 6.158<br>7.112 to 7.121 | |
| GR15 | **Testing and testability during operation**<br>Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis. | 6.159 to 6.191 | |
| GR16 | **Maintainability**<br>The principle of designing I&C systems and equipment important to safety to facilitate timely replacement, repair and adjustment of malfunctioning equipment. | 6.192 to 6.197 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| GR17 | **Provisions for removal from service for testing or maintenance**<br>When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of any protection system bypasses that are necessary for the duration of the testing or maintenance activities. | 6.198 to 6.204 | |
| GR18 | **Setpoints**<br>The requirements and operational limits and conditions established in the design for the nuclear power plant shall include limiting settings for safety systems. | 6.205 to 6.212 | |
| GR19 | **Marking and identification of items important to safety**<br>A consistent, coherent and easily understood method of naming and identifying all I&C components and for use as descriptive titles for the human-machine interface should be determined and followed throughout the design, installation and operation stages in the lifetime of the plant. | 6.213 to 6.219 | |

## 7. DESIGN GUIDELINES FOR SPECIFIC I&C SYSTEMS AND EQUIPMENT

The objective of the system review is to address specific types of I&C systems and equipment, based on the recommendations of Section 7 "*Design guidelines for specific I&C systems and equipment"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SR1 | **Sensing devices**<br>These field devices provide measurements of (1) analogue values of variable or (2) detection of discrete states, such as those detected by limit switches, auxiliary relay contacts and temperature, pressure, flow or level switches. | 7.1 to 7.9 | Sensor measurements of plant physical variables should be consistent with the requirements of the design bases for the I&C systems and the plant. |
| SR2 | **Control systems**<br>The automatic control that maintains the main process variables within operational limits is part of the defence in depth of the plant, and therefore the control systems concerned are normally important to safety. | 7.10 to 7.14 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SR3 | **Protection system**<br>A system that monitors the operation of a reactor and, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition. | 7.15 to 7.59 | |
| SR4 | **Automatic safety actions**<br>Means provided to automatically initiate and control all safety actions of the protection system except those for which manual action alone has been justified.<br>**Manual safety actions**<br>Means provided to manually initiate the safety systems and the individual components that are necessary to initiate and control performance of their safety functions. | 7.18 to 7.26 | |
| SR5 | **Information display**<br>Part of the protection system that makes relevant information available to the operator for monitoring the effects of automatic actions. | 7.27 to 7.28 | |
| SR6 | **Sensors**<br>The sensors that provide signals to the protection system should feed other systems only through appropriate buffering and isolation devices.<br>**Settings**<br>The protection system should provide a means for determining the setpoint values for each channel of the protection system. | 7.29 to 7.34 | |
| SR7 | **Operational bypasses**<br>Operational bypasses or trip conditioning logic are necessary to inhibit the actuation of protection system functions during specific plant conditions. | 7.35 to 7.38 | |
| SR8 | **Latching of protection system functions**<br>Actions initiated by the protection system should be latched so that once an action is started, it will continue until all actions performed by that function are completed, although the initiating state might have ceased to be present. | 7.39 to 7.45 | |
| SR9 | **Spurious initiation**<br>The design of the protection system should, to the extent practicable, minimize the potential for spurious initiation or action of the protection system. | 7.46 to 7.49 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SR10 | **Interaction between the protection system and other systems**<br>Interference between protection systems and control systems at the NPP must be prevented by means of separation, by avoiding interconnections or by suitable functional independence. If signals are used in common by both a protection system and any control system, separation must be ensured and the signal system must be classified as part of the protection system. | 7.50 to 7.59 | |
| SR11 | **Power supplies**<br>Power supplies for I&C systems, irrespective of their type should have requirements on their safety class, reliability provisions, qualification, isolation, testability, maintainability and indication of removal from service that are consistent with the reliability requirements of the I&C systems they serve. | 7.60 to 7.65 | |
| SR12 | **Digital systems**<br>Digital systems include computer based systems and systems programmed with hardware description languages. | 7.66 to 7.147 | If a system important to safety at the NPP is dependent on computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software must be established and implemented throughout the service life of the system and, in particular, throughout the software development cycle. |
| SR13 | **Digital system functions**<br>They provide flexibility to perform complex tasks, improved plant monitoring and improved interfaces with operators, capability for self-test and self-diagnostics, a better environment to facilitate the feedback of operating experience based on data recording, low physical size and low cabling needs. | 7.68 to 7.78 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SR14 | **Digital data communication**<br>This covers all types of communication, including point to point, serial and network communication. | 7.79 to 7.94 | (1) The data communication for safety systems should be designed to have deterministic transmission times.<br>(2) If the communication of safety related data malfunctions in any way, the safety system should continue to perform its safety function or go to a safe state. |
| SR15 | **Independence of data communications**<br>The objective is to prevent common cause failure of safety systems due to data communication. | 7.95 to 7.100 | The topology of the data communication network and access control to media should be designed and implemented in a way that it supports the avoidance of common cause failure of safety systems. |
| SR16 | **Computer security** | 7.101 to 7.130 | Nuclear safety measures and nuclear security measures shall be designed and implemented in an integrated manner so that they do not compromise one another. The use of active computer security features should be considered for detecting computer security threats and mitigating their effects.<br><br>See MS4. |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SR17 | **Devices configured with hardware description languages (HDL)**<br>Devices configured with hardware description languages are programmable electronic modules providing logic structures (e.g. arrays of gates and switches) that are customized by the I&C developer to provide specific functions. Field programmable gate arrays are a common example of devices in this class. | 7.131 to 7.147 | |
| SR18 | **Software tools**<br>Software tools are used to support all aspects of the I&C development lifecycle where benefits result through their use and where such software tools are available. | 7.148 to 7.164 | |
| SR19 | **Qualification of industrial digital devices of limited functionality for safety applications**<br>Devices that have not been developed specifically for use in NPP safety systems and such applications. | 7.165 to 7.175 | |

## 8. CONSIDERATIONS RELATING TO THE HUMAN-MACHINE INTERFACE

The objective of the system review is to assess compliance with the recommendations of Section 8 "*Considerations relating to the human-machine interface"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| | **Human-machine interface**<br>The interface between operating staff and I&C systems and computer systems linked with the plant. The interface includes displays, controls and the interface with the operator support system. | | |
| HM1 | **Main control room**<br>Room from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions. | 8.1 to 8.12 | |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| HM2 | **Supplementary control room**<br>Room that is physically, electrically and functionally separate from the main control room and so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the main control room. | 8.13 to 8.18 | |
| HM3 | **Accident monitoring**<br>Capability based on human-machine interface equipment for monitoring the status of essential equipment and the course of accidents, for predicting the locations of release and the amount of radioactive material that could be released from the locations that are so intended in the design and for post-accident analysis. | 8.19 to 8.35 | |
| HM4 | **Operator communications systems**<br>Communications capabilities provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and are available for use following all postulated initiating events and in accident conditions. | 8.36 to 8.46 | |
| HM5 | **General principles relating to human factors engineering for I&C systems**<br>**Human factors engineering**<br>Engineering in which factors that could influence human performance are taken into account. | 8.47 to 8.93 | |
| HM6 | **Recording of historical data** | 8.94 | |

## 9. SOFTWARE

The objective of the system review is to assess compliance with the recommendations of Section 9 "*Software"* of SSG–39 [1].

**Possible subjects for the IERICS mission**

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SW1 | **Software**<br>Processing instructions and services implemented on programmable or programmed devices. Software types include operating systems, predeveloped software or firmware, software to be specifically developed for the project, or software to be developed from an existing predeveloped family of hardware or software modules. | 9.1 to 9.5 | Examples of software components are source code and executable code, hardware description language, field programmable gate array (FPGA) configuration data (known as 'bit stream') and software that is installed in plant equipment, including applications software, operating systems and support software. |
| SW2 | **Software requirements**<br>Requirements specific to software that are necessary to satisfy I&C system / function requirements. Software requirements describe what the software component must do in order that, when that software is executed on the chosen set of digital equipment, the overall I&C system requirements are met. Software requirements are established early in the software life cycle. | 9.6 to 9.15 | |
| SW3 | **Software design**<br>The allocation of software requirements and functionality into an organized set of interacting software components and the detailed description of those components. | 9.16 to 9.43 | The design should demonstrably address all software requirements and should not contain any unsafe or unnecessary functionality. The design will normally address the architecture of the software and the detailed design within that architecture. |

| Id. | Topic and description | SSG–39 clauses | Remark |
|---|---|---|---|
| SW4 | **Software implementation**<br>The realization of software design in executable form. The implementation instantiates the internal software design and interfaces into specific software components. The resulting output includes source and executable code, logic and test results. | 9.44 to 9.63 | The software implementation should demonstrably address all software requirements and the software design. |
| SW5 | **Software verification and analysis**<br>Verification consists of confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity. This activity includes testing and analysis. | 9.64 to 9.95<br>2.66 to 2.74<br>7.148 to 7.164 | The result of this activity should be a coherent set of evidence that the software requirements, design and implementation are complete, correct and consistent. |
| SW6 | **Predeveloped software**<br>Software that already exists, is available as a commercial or proprietary product and is being considered for use in an I&C system. | 9.96 to 9.98<br>2.108 to 2.117 | |
| SW7 | **Software tools**<br>Tools that support the I&C development life cycle. They are typically used to control the issue of modules for assembly into system components and to control the software build used for system validation. Software tools are also used onsite in operation to facilitate configuration control and traceability between installed components and validated components. | 9.99<br>7.148 to 7.164 | See also SR18. |
| SW8 | **Third party assessment**<br>An independent assessment of the adequacy of the system and its software. Such an assessment typically involves an examination of both the development process and final software. | 9.100 to 9.103 | |

## 10. OPERATION & MAINTENANCE PROCESSES REVIEW

The objective of the operation & maintenance review is to determine whether the corresponding processes applied by the counterpart comply with the review basis and reference and the best international practices.

The table below contains topics that are not fully covered by SSG–39 [1] but may be of interest to counterparts of the review mission.

**Possible subjects for the IERICS mission**

| Id. | Topic and Description | | Remark |
|---|---|---|---|
| OM1 | **System operation procedures** | | |
| OM2 | **Maintenance procedures** | | |
| OM3 | **Periodic testing procedures** | | |
| OM4 | **Training**<br>of operation and maintenance personnel. | | |
| OM5 | **Failure detection and reporting** | | |

# APPENDIX II

# MISSION REPORT TEMPLATE

This appendix provides information that may be used by the IERICS team as a template for the mission report. It is available in electronic form. On the following pages the text in italics should be replaced with the attributes of the given IERICS mission.

IERICS-*LOCATION*-20*XX*
*???* version
Original: English
Distribution: Restricted

**INTERNATIONAL ATOMIC ENERGY AGENCY**

# MISSION REPORT

# INDEPENDENT ENGINEERING REVIEW OF INSTRUMENTATION AND CONTROL SYSTEMS (IERICS)

# IAEA REVIEW OF
# *(Review Mission Title)*

***(Review Location)***

***(Review Mission Period)***
***(Follow-up Mission Period)***

IERICS

IAEA REVIEW OF *Title of System Reviewed*

IAEA DEPARTMENT OF NUCLEAR ENERGY
DIVISION OF NUCLEAR POWER

**(FINAL) MISSION REPORT**

# INDEPENDENT ENGINEERING REVIEW OF INSTRUMENTATION AND CONTROL SYSTEMS (IERICS)

# IAEA REVIEW OF

*(Review Mission Title)*

***(Graphic of the plant or system may be added on this page)***

**REPORT TO**
***Counterpart organization***

***(Review mission period)***
***(Review location)***
***(Follow-up mission period)***
***(Review location)***

**(FINAL) MISSION REPORT**

# INDEPENDENT ENGINEERING REVIEW OF INSTRUMENTATION AND CONTROL SYSTEMS (IERICS)

# IAEA REVIEW OF

*(Review Mission Title)*

| | | |
|---|---|---|
| **Mission date:** | *Review period* | |
| **Location:** | *Location of review* | |
| **Facility:** | *Counterpart organization* | |
| **Organized by:** | International Atomic Energy Agency (IAEA)<br>Department of Nuclear Energy<br>Division of Nuclear Power | |
| **IAEA review team:** | *Participant Name* | *(Organization, Country)* |
| | *Participant Name* | *(Organization, Country)* |
| **Follow-up mission date:** | *Review period* | |
| **Mission location:** | *Review period* | |
| **IAEA review team:** | *Participant Name* | *(Organization, Country)* |
| | *Participant Name* | *(Organization, Country)* |

Issued on *date*

## CONTENTS

# EXECUTIVE SUMMARY

In 2009, the Nuclear Power Engineering Section of the IAEA established the Independent Engineering Review of I&C Systems (IERICS) mission to conduct peer reviews of design documents, prototype systems and systems in actual operation in nuclear power plants (NPPs). This report documents the IERICS review performed during the days of *review period and review location, on the system(s) being reviewed*.

The IERICS mission is conducted by a team of international experts with direct experience applicable to the areas of the review. Judgements of compliance are made on the basis of IAEA publications and of the combined expertise and experience of the international review team. The review is not a regulatory inspection or audit against national or international codes and standards. The mission is a peer review, the results of which can be used to make improvements in the various processes, such as design, testing, implementation, licensing, operation and maintenance.

Background of the system(s) being reviewed.

*History of the review request and the discussion of the preparatory meeting and the basis for the review such as* ….The present review was based on the guidance defined in the IAEA Safety Guide SSG–39 entitled "Design of Instrumentation and Control Systems for Nuclear Power Plants" [1] and related IAEA Nuclear Safety and Nuclear Energy Series publications [ref]. Additionally, the guidelines of the IAEA TECDOC on "Preparing and Conducting Review Missions of Instrumentation and Control Systems in Nuclear Power Plants, IAEA TECDOC–1662, Rev. 1." [17] were followed. The IERICS review was performed by a group of invited subject matter experts. The results of their review were published in the present mission report at the end of the review. It provides recommendations, suggestions and comments as well as notes good practices on the design and in the design process.

*Goals of the counterpart organization*….such as their goals were that the mission would provide them with a basis for improving the technical design, safety features and reliability of the counterpart's I&C system by implementing the recommendations and suggestions of the mission and would also assist in meeting the requirements of the future implementations.

*Description of the general manner as to how the review was conducted such as* The IERICS activities consisted of a series of formal presentations by counterpart organization staff (supported by associated organizations), clarification discussions between the IAEA review team and the counterpart after these presentations, as well as a tour of the facilities. Prior to the review mission, *counterpart* compiled an Advance Information Package (AIP), which the team members reviewed carefully and submitted a series of written questions to the designers. These were followed-up by oral presentations and subsequent discussions between the two parties. The IAEA review team submitted written questions to *counterpart* also during the course of the mission, which were then similarly addressed in follow-up discussions.

The conclusions of this report summarize the findings of the review mission and provide *number (99)* recommendations and *number (99)* suggestions for the counterpart to consider along with acknowledging *number (99)* good practices from which other organizations may benefit.

Through the review of the presented documents and discussions with the counterparts, the IAEA review team confirmed that extensive engineering work of high quality has been performed to develop the system under review. Based on an assessment of adherence to safety recommendations in the relevant sections of the IAEA Safety Guide SSG–39, the reviewed parts of the I&C systems *(or the I&C platform and aspects of its application as safety systems)* were generally found to be in compliance. Specific issues, identified as areas for further improvement, are listed in the issue sheets as recommendations and suggestions.

*If deemed appropriate by the review team, text similar to the following may be used in the report….*

It should be noted that modern digital monitoring and control systems, such as those of the system under review, are extremely complex systems and the review mission was conducted for only a relatively short time period. It is the opinion of the review team that some comments in the report may not be seen as deficiencies in the design or the design process, but may be a result of the difficulty in resolving all of their concerns in such a limited time period.

*A paragraph to be added on the follow-up mission may include a summary such as….*

In *year/company* requested the IAEA to perform a follow-up IERICS review. The detailed scope and work plan for this follow-up mission was established in a preparatory meeting at *the ..., on ..date*. The follow-up mission took place *on ..date, location*. During the course of the mission, the counterpart actions in response to all recommendations, suggestions and comments from the main mission were overviewed. *Counterpart* introduced their action plan and the projected completion date for the remaining open issues. Based on the findings of the follow-up mission, all issue sheets were updated with the final assessment by the IAEA review team and the sheets were closed. No further recommendations or suggestions were raised.

# DISCLAIMER

The assessment provided here, describing issues and good practices, represents the opinion of the expert team, and does not constitute recommendations or suggestions made by the IAEA or made on the basis of a consensus of IAEA Member States.

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person. Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of the report.

The mention of names of specific companies or products in this report 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.

# 1. INTRODUCTION

## 1.1. BACKGROUND OF THE MISSION

A review mission titled "Independent Engineering Review of Instrumentation and Control Systems" (IERICS) in nuclear power plants (NPPs) was established in 2009 at the Nuclear Power Engineering Section of the IAEA. The mission is intended to conduct peer reviews of design documents, prototype systems and systems in actual operation in NPPs. The IERICS mission is performed by a group of invited subject matter experts from various IAEA Member States. The IERICS mission is based on appropriate IAEA documents, such as Safety Guides and Nuclear Energy Series Reports.

*This portion may be tailored based on the results of the preparatory meeting….*

The guidelines for the current IERICS mission were established at a preparatory meeting in *location and date of the preparatory meeting*.

### 1.1.1 Review bases

Besides the recommendations from designated *name of standards and [refs]* and the IAEA TECDOC on "Preparing and Conducting Review Missions of Instrumentation and Control Systems in Nuclear Power Plants", IAEA TECDOC–1662, Rev. 1. [ref], the review methodology followed the structure of the IAEA Safety Guide SSG–39, titled "Design of Instrumentation and Control Systems for Nuclear Power Plants" [1]. More specifically, the following areas were used as criteria in the review *(delete clauses that do not apply)*:

SECTION 2. THE MANAGEMENT SYSTEM FOR I&C DESIGN

—Use of life cycle models:
- Process planning;
- Coordination with human factors engineering activities and computer security activities.

—Activities common to all life cycle phases:
- Configuration management;
- I&C systems hazard analysis;
- Verification and validation;
- Use of insights from probabilistic safety analysis;
- Safety assessment;
- Documentation.

—Life cycle activities:
- Requirement specification;
- Selection of pre-developed items;
- Design and implementation of I&C systems;
- System integration;
- System validation;
- Installation, overall I&C integration and commissioning;
- Operation and maintenance;
- Modifications.

SECTION 3. DESIGN BASIS FOR I&C SYSTEMS

—Identification of I&C functions;
—Content of design basis for I&C systems.

SECTION 4. I&C ARCHITECTURE

—Architectural design;
—Content of the overall I&C architecture;
—Content of individual I&C system architectures;
—Independence;
—Consideration of common cause failure.

SECTION 5. SAFETY CLASSIFICATION OF I&C FUNCTIONS, SYSTEMS AND EQUIPMENT

SECTION 6. GENERAL RECOMMENDATIONS FOR ALL I&C SYSTEMS IMPORTANT TO SAFETY

—Design for reliability:
- Single failure criterion;
- Redundancy;
- Independence;
- Diversity;
- Failure modes.

—Equipment qualification:
- Suitability and correctness;
- Environmental qualification;
- Internal and external hazards.

—Design to cope with ageing and obsolescence;
—Control of access to systems important to safety;
—Testing and testability during operation;
—Maintainability;
—Provisions for removal from service for testing or maintenance;
—Setpoints;
—Marking and identification of items important to safety.

SECTION 7. DESIGN GUIDELINES FOR SPECIFIC I&C SYSTEMS AND EQUIPMENT

—Sensing devices;
—Control systems;
—Protection system:
- Automatic safety actions and manual safety actions;
- Information display;
- Sensors and settings of the protection system;
- Operational bypasses;
- Latching of protection system functions;

- Spurious initiation;
- Interaction between the protection system and other systems.

—Power supplies;

—Digital systems:

- Digital system functions;
- Digital data communication;
- Independence of data communications;
- Computer security;
- Devices configured with hardware description languages.

—Software tools;

—Qualification of industrial digital devices of limited functionality for safety applications.

SECTION 8. CONSIDERATIONS RELATING TO THE HUMAN-MACHINE INTERFACE

—Control rooms;

—Accident monitoring;

—Operator communications systems;

—General principles relating to human factors engineering for I&C systems;

—Recording of historical data.

SECTION 9. SOFTWARE

—Software requirements;

—Software design;

—Software implementation;

—Software verification and analysis;

—Predeveloped software;

—Software tools;

—Third party assessment.

*Number (99)* specific topics listed above were selected for the review.

### 1.1.2 Product background

*A short summary of the product background may follow here.*

## 1.2. OBJECTIVE AND SCOPE OF THE MISSION

The objectives of the IERICS review mission were:

—To conduct an independent and comprehensive review of the technical information provided by the counterpart in accordance with the recommendations of the IAEA Safety Guide SSG–39;

—To produce a mission report at the end of the review, including issue sheets and good practice sheets.

The following subjects were requested by *counterpart* to be reviewed by the IERICS team with respect to *development process and history, design, system characteristics, functionality and operational performance*:

—System, process and/ or component 1;
—System, process and /or component 2…;
—System, process and/ or component n.

Additional areas to be consulted on were:

—System, process and/ or component a;
—System, process and /or component b…;
—System, process and/ or component z.

It was the counterpart organization's expectation that the findings of IAEA's IERICS review, as an independent international technical review, will provide the following benefits to their development project:

—To enhance the technical design, safety features and reliability of the *system(s) under review* by implementing the recommendations and findings of the mission;
—Other (non-commercial, business or marketing oriented) expectations of the counterpart.

## 1.3. BASIS AND REFERENCE FOR THE REVIEW

### 1.3.1 Guideline reference to conduct the review

The basis for the review was the IAEA Safety Guide SSG–39 [1] and related IAEA Nuclear Safety and Nuclear Energy Series publications [ref]. *In addition, recommendations of the IAEA Safety Guide SSG–39 were further explained and clarified using a number of IEC Standards (or other references) [ref].* The review team members also used their expert judgments to compare the review subjects against existing international good practices.

### 1.3.2 Information reviewed

The information provided by *counterpart* for the review purposes was supported by the following documents and presentations:

| Item No. | Title | Revision (date) | Page |
|---|---|---|---|
| Advance Information Package (AIP) | | | |
| 1. | *Listing of review basis documents…* | | |
| 2. | | | |
| Presentations and documents provided during the IERICS mission | | | |
| 1. | *Listing of review basis documents and presentations…* | | |
| 2. | | | |

## 1.4. CONDUCT OF THE REVIEW

The IERICS review mission was conducted based on the technical information provided by *counterpart* in the following forms:

- An advance information package (AIP) consisting of *(99) number of volumes or sections* introducing the *name of the system*, including its constituent modules, subsystems and systems. (The questions and comments compiled by the review team prior to the mission on *the counterpart*'s AIP consisted of *NN general remarks and questions, XX specific requests for more detailed information, YY questions and comments regarding compliance with IAEA SSG-39 as well as ZZ specific* items. The list can be found in Appendix V of this report.);
- Presentations by counterpart experts *and representatives of other companies*, delivered during the course of the mission, and listed in Section 1.3.2;
- Printed review materials and demonstrations and tours held during the review process;
- *As required…* Additional presentations and discussions, including the counterpart's response to questions and requests compiled by the review team during the course of the mission. (*The list of XX general and YY specific* questions can be found in Appendix VI of this report.)

Counterparts from *counterpart*, as the component designer of the advanced I&C system, and additional counterparts from participating organizations were involved in the technical meetings and discussions. The list of all participants can be found in Appendix I of this report.

The counterpart organization was well prepared and presentation materials were comprehensive and well presented.

*Discussion of any tours and/or demonstrations during the review follows…*

Assessment of the contents and compliance of the design have been carried out based mainly on comparison to the IAEA Safety Guide SSG–39, as well as international good practices, with the purpose of identifying strong points and opportunities for improvement.

The conclusions, recommendations, suggestions, comments and good practices (documented in Sections 3.2., 3.3. and Appendices III to IV of this report) were presented and agreed upon with the counterpart during the close-out meeting.

*One or two paragraphs to be added on the follow-up mission may include a summary such as….*

During the course of the follow-up mission *in location, dates*, the counterpart actions, intermediate results and documents in response to all recommendations, suggestions and comments from the main mission were overviewed. *Counterpart* introduced their action plan and the projected completion date for issues that have not been fully closed yet. The planned actions are primarily focused on improvements in design processes and enhancements of the technical solutions.

Based on the findings of the follow-up mission, all issue sheets were updated with the final assessment by the IAEA review team and the sheets were closed. No further recommendations or suggestions were raised.

This report is a joint effort of the IAEA review team at large. Its content was shared among all the review team members and consensus agreement was achieved.

The review was conducted in an excellent atmosphere of mutual understanding with a positive sharing of experience between the team members and the counterpart.

## 1.5. CONTENT OF THE MISSION REPORT

Section 1 of the report provides general mission information. Section 2 describes the assessment methodology and provides an outline of the findings in each area reviewed. Section 3 provides a summary with general conclusions, a list of specific recommendations, suggestions and comments or observations, as well as a list of good practices.

Appendices I and II of the report provide the list of participants to the meetings and the agenda of the main and the follow-up missions.

Detailed technical recommendations and suggestions in the form of issue sheets developed by the IAEA experts are collected in Appendix III, while identified good practices are presented in detail in Appendix IV. Appendix V lists the preliminary questions and comments put by the IAEA review team on *counterpart*'s Advance Information Package (AIP). Appendix VI lists questions and requests for additional explanation put by the IAEA review team during the course of the mission.

# 2. ASSESSMENT OF THE ISSUES

## 2.1. PRESENTATION AND TREATMENT OF THE ISSUES

### 2.1.1 General

In this section, the prepared format is described for documenting the issues and good practices that have been identified by the IERICS team.

The issues are presented in sequence and numbered, with an issue sheet specific for each issue. Each issue sheet consists of the following sections:

For the main review mission on the subject:

(1) Issue identification;
(2) Issue clarification;
(3) Counterpart view on the issue (optional);
(4) Assessment by the IAEA review team;
(5) Counterpart response on the recommendations / suggestions (optional).

For the follow-up missions on the same subject:

(6) Counterpart actions taken after the mission;
(7) Follow-up assessment by the IAEA review team.

(Clarification: for each follow-up mission, new sections of (6) and (7) may be added.)

In the "Issue clarification" section of each issue sheet, a clear reference to the relevant recommendation of IAEA Safety Guide SSG–39 used in the review is indicated.

If, as an outcome of a follow-up mission, a new design issue appears with respect to the previous ones, a new issue sheet is generated.

### 2.1.2 Comments on Sections 3, 5 and 6 of the issue sheet

The purpose of Sections 3, 5 and 6 of the issue sheets is to reflect the views of and the measures taken by the counterpart for the issue resolution, including the self-assessment.

### 2.1.3 Comments on Sections 4 and 7 of the issue sheet

The purpose of Sections 4 and 7 of the issue sheets is to reflect the discussions with the counterpart experts, to record the conclusions, to issue possible recommendations and suggestions and to synthesize the experts' judgment on the resolution of the design issue under discussion.

In these sections, included are the findings, comments, recommendations and suggestions resulting from the IAEA review team's assessment. They are provided on the basis of the following criteria:

**Suggestions and recommendations:** These give advice from the external experts of the IAEA review team to the counterpart and they are provided in order to resolve a deviation from the IAEA safety guide and/or from the internationally recognized good practices in the subject.

**(1) Recommendations** Follow-up action is required to resolve a deviation from the IAEA safety guide and/or internationally recognized good practices by making improvements, or by establishing a plan for making improvements, or resolving the issue by other means.

**(2) Suggestions** Follow-up action is not strictly required: it is only optional in order to get closer to internationally recognized good practices.

**Comments:** They are observations of the review team that are provided for information only. No action or response is required on the counterpart side.

Recommendations and suggestions are numbered in sequential order for further reference. The reviewed documents, corresponding specifically to the issue under consideration, are also listed in the issue sheets.

### 2.1.4 Summary of the identified issues

The following table summarizes the issues.

| Issue No. | Title of issue | Recommendation No. | Suggestion No. |
|---|---|---|---|
| I1-*AAA* | *Text from Section 1 of the issue sheet I1-AAA* | *Applicable R# (if one exists)* | *Applicable S# (if one exists)* |
| I2-*BBB* | *Text from Section 1 of the issue sheet I2-BBB* | *Applicable R# (if one exists)* | *Applicable S# (if one exists)* |
| **Total** | ***# of issue sheets*** | ***# of recommendations*** | ***# of suggestions*** |

All the issue sheets are collected in Appendix III.

## 2.2. PRESENTATION OF GOOD PRACTICES

In this section of the report, the good practices identified by the IAEA review team are presented, following a prepared format for the good practices.

The good practices are presented in sequence and numbered, with a good practice sheet specific for each item.

Each good practice sheet consists of the following sections:

(1) Good practice identification;
(2) Good practice clarification;
(3) Counterpart view on the identified good practice (optional);
(4) Assessment by the IAEA review team.

The following table summarizes the identified good practices.

| GP No. | Title of good practice |
|---|---|
| *GP-1* | *Text from Section 1 of the good practice sheet GP1* |
| *GP-2...* | *Text from Section 1 of the good practice sheet GP2* |
| *GP-n* | *Text from Section 1 of the good practice sheet GPn* |

All the good practice sheets are collected in Appendix IV. These practices may be considered and may serve as good engineering examples for other nuclear power plant I&C system design projects.

# 3. MAIN CONCLUSIONS AND RECOMMENDATIONS

## 3.1. GENERAL CONCLUSION

*Remarks in the conclusions will be dependent on the observations made during review but a suggested format is…*

Through the review of the presented documents and discussions with the counterparts, the IAEA review team confirmed that extensive engineering work of high quality has been performed to develop the advanced I&C systems for *system(s) under review*. In general, the reviewed parts of the I&C system are consistent with the requirements of the relevant sections of IAEA Safety Guide SSG–39. Specific issues, identified as areas for further improvement, are listed in the issue sheets, as suggestions and recommendations. *The issue sheets were updated and closed based on the findings of the follow-up mission.*

### 3.1.1 Review of the systems / presented documents

The scope of the review covered (as appropriate):

—Review area 1;
—Review area 2...;
—Review area n.

*3.1.1.1. Review area 1*

*Discussion of review area 1*

*3.1.1.2. Review area 2*

*Discussion of review area 2*

*3.1.1.3. SSG-39 compliance assessment*

*Discussion of compliance with SSG-39 recommendations*

### 3.1.2 Description of tours and/or demonstrations held during the review

The visited areas covered:

—Review area 1;
—Review area 2...;
—Review area n.

The visit helped the review team to understand the *design, preparation, implementation, operation and testing of the reviewed I&C systems, including the underlying I&C platforms*.

## 3.2. SPECIFIC RECOMMENDATIONS / SUGGESTIONS / COMMENTS

After the review and discussion with the counterparts, the IAEA review team compiled *(99) number* recommendations, *(99) number* suggestions and *(99) number* comments (See Appendix III for more details.)

### 3.2.1 Recommendations

***R1)*** *Text of recommendation 1;*
***R2)*** *Text of recommendation 2.*

### 3.2.2 Suggestions

***S1)*** *Text of suggestion 1;*
***S2)*** *Text of suggestion 2.*

### 3.2.3 Comments / observations

***C1)*** *Text of comment 1;*
***C2)*** *Text of comment 2.*

## 3.3. GOOD PRACTICES

After the review and discussion with the counterpart, the IAEA review team compiled *(99) number* good practices (See Appendix IV for more details.)

***GP1)*** *Text of good practice 1;*
***GP2)*** *Text of good practice 2.*

# ACKNOWLEDGEMENT

*Tailored based on how the review went….*

The host organization provided excellent conditions for conducting the mission. The counterpart organization staff was fully prepared for the technical discussions, presentations and demonstrations, and they promptly and properly responded to the questions and clarification requests from the IAEA review team.

# REFERENCES

*Update the list according to actual mission review basis*

IAEA SAFETY STANDARDS SERIES:

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

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

[3] 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).

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

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

IAEA NUCLEAR ENERGY SERIES

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementing Digital I&C Systems in the Modernization of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-1.4, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Protecting Against Common-Cause Failures in Digital I&C Systems, IAEA Nuclear Energy Series No. NP-T-1.5, IAEA, Vienna (2009).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Integration of Analog and Digital Instrumentation and Control Systems in Hybrid Control Rooms, IAEA Nuclear Energy Series No. D-NP-T-3.10, IAEA, Vienna (2010).

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

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

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.17, IAEA, Vienna (2016).

IAEA TECHNICAL DOCUMENTS (TECDOC)

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance, IAEA-TECDOC-1402, IAEA, Vienna (2004).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Managing Modernization of Nuclear Power Plant Instrumentation and Control Systems, IAEA-TECDOC-1389, IAEA, Vienna (2004).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Solutions for Cost Effective Assessment of Software Based Instrumentation and Control Systems in Nuclear Power Plants, IAEA-TECDOC-1328, IAEA, Vienna (2003).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparing and Conducting Review Missions of Instrumentation and Control Systems in Nuclear Power Plants, IAEA-TECDOC-1662 Rev. 1., IAEA, Vienna (2016).

# ABBREVIATIONS USED IN THE MISSION

*(List should be tailored for the review…)*

| | |
|---|---|
| CCF | common cause failure |
| CEA | control element assembly |
| CH | channel |
| COTS | commercial off the shelf |
| CPLD | complex programmable logic device |
| CPS | computerized procedure system |
| CRCS | control rod control system |
| DCS | digital control system |
| DDS | document delivery schedule |
| DPS | diverse protection system |
| EMI | electromagnetic interference |
| EQ | equipment qualification |
| ESF | engineered safety features |
| EWS | engineering workstation |
| FMEA | failure mode and effect analysis |
| FPGA | field programmable gate array |
| I&C | instrumentation and control |
| IAEA | International Atomic Energy Agency |
| IEC | International Electrotechnical Commission |
| IERICS | independent engineering review of instrumentation and control systems |
| IT | information technology |
| MCR | main control room |
| MMI | man machine interface |
| MMIS | man machine interface system |
| MTBF | mean time between failures |
| MTP | maintenance and test panel |
| MTTR | mean time to repair |
| NPP | nuclear power plant |
| PAMI | post-accident monitoring instrumentation |
| PCM | power converter module |
| PLC | programmable logic controller |
| PLD | programmable logic devices |
| PPS | plant protection system |
| QA | quality assurance |
| R&D | research and development |
| RPS | reactor protection system |
| RTM | requirements traceability matrix |
| SDN | safety data network |
| SER | safety evaluation report |
| SFC | single failure criterion |
| SPV | single point vulnerability |
| SW | software |
| TR | technical report |
| TTL | transistor-transistor-logic |
| V&V | verification and validation |

# APPENDIX I
# LIST OF PARTICIPANTS

## I. IAEA review team

*(1) Reviewer 1 IAEA/NENP, Team leader*
*(2) Reviewer 2 Organization, country*
*(3) Reviewer n Organization, country*

## II. Counterpart participants

*(1) Participant 1 Title/Organization*
*(2) Participant 2 Title/Organization*
*(3) Participant n Title/Organization*

# APPENDIX II
# MAIN MISSION PROGRAMME

*Agenda/Timetable of the review meeting*

# FOLLOW-UP MISSION PROGRAMME

*Agenda/Timetable of the follow-up meeting*

# APPENDIX III
# ISSUES

*Insert issue sheets in sequential order I1, I2,...*

| ISSUE SHEET #X | |
|---|---|
| **1. ISSUE IDENTIFICATION** | Issue number: |
| Mission: | **IAEA REVIEW OF THE *SYSTEM TITLE*** |
| Reviewed area: | |
| Issue title: | |

| **2. ISSUE CLARIFICATION** | **Date:** |
|---|---|
| **2.1 - ISSUE DESCRIPTION** | |
| **2.2 – IDENTIFIED BY:** | **Review team ☐** **Counterpart ☐** |
| **2.3 – ISSUE CREATED BASED ON THE FOLLOWING DOCUMENTS / PRESENTATIONS PROVIDED BY THE COUNTERPART:** | |
| **2.4 - REFERENCE TO IAEA AND OTHER RELEVANT DOCUMENTS** | |

| **3. COUNTERPART VIEW ON THE ISSUE (OPTIONAL)** |
|---|
| |

| **4. ASSESSMENT BY THE IAEA REVIEW TEAM** |
|---|
| **4.1 – COMMENTS:** |
| **4.2 – RECOMMENDATIONS AND SUGGESTIONS:** |

| **5. COUNTERPART RESPONSE ON THE RECOMMENDATIONS / SUGGESTIONS (OPTIONAL)** |
|---|
| |

**FOLLOW UP** *(if required)*

| **6. COUNTERPART ACTIONS TAKEN AFTER THE MISSION** | **Date**: |
|---|---|
| | |

| **7. FOLLOW-UP ASSESSMENT BY THE IAEA REVIEW TEAM** | **Date:** |
|---|---|
| **7.1 - COMMENTS:** | |
| **7.2. RECOMMENDATIONS AND SUGGESTIONS:** | |
| **7.3 - DOCUMENTS REVIEWED:** | |

| **STATUS OF THE ISSUE** | | | **Date:** |
|---|---|---|---|
| ***Resolution degree:*** | | | |
| **1** | **No action** | *The issue was not agreed on by the counterpart and no action was taken to resolve it. No progress in the resolution of the issue, or unsatisfactory resolution.* | |
| **2** | **Action planned or under way** | *The issue was agreed on by the counterpart, but the solution is unidentified or is being defined.*<br>*or*<br>*The issue was agreed on by the counterpart, but the solution has not yet started.*<br>*or*<br>*The issue was agreed on by the counterpart and work has started to resolve it.* | |
| **3** | **Action completed, issue not resolved** | *The issue was agreed on by the counterpart and actions are completed in the counterpart's view. The implemented actions meet only partially or do not meet the intent of the recommendations of the previous IAEA review.* | |
| **4** | **Action completed, issue resolved** | *The issue was agreed on by the counterpart and the solution provided is fully satisfactory. The intent of the recommendations / suggestions of the review is fully met. Issue closed.* | |

# APPENDIX IV
# GOOD PRACTICES

*Insert good practice sheets in sequential order GP1, GP2,...*

| GOOD PRACTICE (GP) SHEET #X | | |
|---|---|---|
| **1. GP IDENTIFICATION** | GP Number: | |
| Mission: **IAEA REVIEW OF THE *SYSTEM TITLE*** | | |
| Reviewed area: | | |
| GP title: | | |

| **2. GP CLARIFICATION** | **Date:** |
|---|---|
| **2.1 - GP DESCRIPTION:** | |
| **2.2 – GP WAS IDENTIFIED BASED ON THE FOLLOWING DOCUMENTS / PRESENTATIONS PROVIDED BY THE COUNTERPART:** | |
| **2.3 - REFERENCE TO IAEA AND OTHER RELEVANT DOCUMENTS:** | |

| **3. COUNTERPART VIEW ON THE IDENTIFIED GP (OPTIONAL)** |
|---|
| |

| **4. ASSESSMENT BY THE IAEA REVIEW TEAM** |
|---|
| **4.1 – COMMENTS (meets expectations of international practices):** ***M1)*** |
| **4.2 – COMMENTS (exceeds expectations of international practices):** ***E1)*** |

# APPENDIX V

## PRELIMINARY QUESTIONS AND COMMENTS ON *COUNTERPART*'S ADVANCE INFORMATION PACKAGE

### General questions

*(1) General question 1.*
*(2) General question n.*

### Detailed questions

*(1) Detailed question 1.*
*(2) Detailed question n.*

# APPENDIX VI

## IAEA REVIEW TEAM QUESTIONS
## REQUESTS FOR ADDITIONAL EXPLANATION

*These are the clarification questions submitted by the review team during the course of the mission, prior to the development of the issue sheets…*

### General questions

*(3) General question 1.*
*(4) General question n.*

### Detailed questions

*(3) Detailed question 1.*
*(4) Detailed question n.*

*Add any other Appendices as needed here after Appendix VI.*

*End of mission report template*

# GLOSSARY

**advance information package**. A set of documents provided to the IERICS team members by the counterpart organization during the preparatory phase prior to the review mission.

**breakout session**. A technical session during the review mission where only a part of the IERICS team is involved.

**briefing meeting**. A meeting of the IERICS team typically held the day prior to the review mission to ensure that all members of the IERICS team have all necessary information and understanding.

**code of conduct**. A set of policies and practices that the IERICS team members must observe during the review mission.

**closeout session**. Final plenary session during the review mission, where the IERICS team presents its findings, the counterpart expresses their point of view and mutual agreement is attained on any remaining outstanding issues.

**comment**. Observations of the IERICS team based on the review and the discussions during the review mission. It is for information only, no action or response is required on the counterpart side.

**counterpart**. Organization that has requested the IERICS mission, that is responsible for providing information and answers necessary to the review and that hosts the review mission.

**counterpart representative**. Person designated by the counterpart to be the counterpart of the IERICS team leader.

**debriefing meeting**. Meeting of the IERICS team held the day after the review mission per se, to develop a quasi-final state for the mission report.

**finding**. Comment, issue, recommendation, suggestion or good practice that the IERICS team mentions, or intends to mention, in the mission report.

**focused review**. Technical session during the review mission that allows the IERICS team to study a selected topic in deep detail.

**good practice**. An outstanding and proven performance, programme, activity or design element, markedly superior to other practices observed elsewhere and not just in its fulfilment of current requirements or expectations.

**IERICS mission**. Engineering review service directly addressing strategy and the key elements for implementation of modern I&C systems, noting in applicable cases, specific concerns related to the implementation of digital I&C systems and the use of software and/or digital logic in safety applications of a NPP.

**IERICS team meeting**. Meeting during the review mission involving the IERICS team only and allowing the team members to share information and understanding, to compare points of view and to reach a team consensus on questions and findings.

**IERICS team leader**. An IAEA staff member designated to be responsible for all preparatory activities, to act as an official liaison with the counterpart, to co-chair the review mission with the counterpart representative, to coordinate the preparation and issuance of the mission report and to be responsible for all follow-up activities.

**issue**. An identified concern or an area for improvement, which has been identified on the basis of the review basis and reference and/or internationally recognized good practices in the subject.

**opening session**. Initial plenary session during the review mission, to make sure that all the participants to the review mission (IERICS team and counterpart) have all necessary or useful information and understanding.

**platform**. A set of hardware and software components that may work cooperatively in one or more defined architectures (configurations). A platform usually provides a number of standard functionalities (e.g. application functions or hardware modules) that may be combined to generate a specific application.

**plenary session**. Session during the review mission involving the complete IERICS team and the counterpart.

**recommendation**. Advice from the IERICS team on what improvements should be made that would contribute to resolve an issue. Usually a recommendation means a non-compliance of a product or a process with IAEA guidance or the internationally recognized good practice. Follow-up action is required.

**review basis and reference**. A set of documents against which the system under review will be assessed.

**suggestion**. Advice from the IERICS team on what improvements may be made that would contribute to resolve an issue. Follow-up action is not strictly required, it is only optional in order to get closer to internationally recognized good practices.

**system under review**. The item to be reviewed, its properties and boundaries.

**technical presentation**. Technical session where the counterpart presents a specific aspect of the system under review, at a level of detail that allow the IERICS team to assess the system's compliance to the review basis and references.

**technical session**. A session during the review mission involving the IERICS team and the counterpart, where the IERICS team reviews specific technical topics.

**technical visit**. Technical session where the IERICS team can collect facts on the ground that would otherwise be difficult to gather from the documentation or presentations.

# ABBREVIATIONS

| | |
|---|---|
| AIP | advance information package |
| I&C | instrumentation and control |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IERICS | independent engineering review of instrumentation and control systems |
| NEPIO | Nuclear Energy Programme Implementing Organization |
| NPP | nuclear power plant |
| V&V | verification and validation |

# CONTRIBUTORS TO DRAFTING AND REVIEW

| | |
|---|---|
| Baeg, S. Y. | Doosan Heavy Industries and Constructions Co., Republic of Korea |
| Bartha, T. | SZTAKI, Hungary |
| Chernyaev, A. | VNIIAES, Russian Federation |
| Eiler, J. | International Atomic Energy Agency |
| Gerasymenko, K. | SRPA “Impulse”, Ukraine |
| Glöckler, O. | International Atomic Energy Agency |
| Harber, J. | Atomic Energy of Canada Limited, Canada |
| Jiang, J. | University of Western Ontario, Canada |
| Johnson, G. | International Atomic Energy Agency |
| Kang, K. S. | International Atomic Energy Agency |
| Kim, J. G. | Korea Hydro & Nuclear Power Co., Republic of Korea |
| Kim, K. H. | Doosan Heavy Industries and Constructions Co., Republic of Korea |
| Kolchev, K. | VNIIAES, Russian Federation |
| Lindner, A. | Industrielle Software-Technik GmbH, Germany |
| Orme, S. | British Energy, United Kingdom |
| Sivokon, V. | JSC ‘Scientific and Engineering Center’, Russian Federation |
| Sklyar, V. | RADIY, Ukraine |
| Nguyen, T. | Électricité de France, France |
| Wood, R.T. | Oak Ridge National Laboratory, United States of America |

**Consultants Meetings**

Vienna, Austria: 12–14 January 2010, 4–7 May 2010, 16–19 November 2015

IAEA
International Atomic Energy Agency

No. 24

# ORDERING LOCALLY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**JAPAN**
***Maruzen-Yushodo Co., Ltd.***
10-10, Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: http://maruzen.co.jp

**RUSSIAN FEDERATION**
***Scientific and Engineering Centre for Nuclear and Radiation Safety***
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: http://www.secnrs.ru

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

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

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

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

International Atomic Energy Agency
Vienna
ISBN 978–92–0–105816–4
ISSN 1011–4289