

IAEA Safety Standards

for protecting people and the environment

Design of Instrumentation and Control Systems for Nuclear Power Plants

Specific Safety Guide

No. SSG-39



IAEA

International Atomic Energy Agency



Documents

Document Sharing Hub

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available on the IAEA Internet site

<http://www-ns.iaea.org/standards/>

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

DESIGN OF INSTRUMENTATION
AND CONTROL SYSTEMS FOR
NUCLEAR POWER PLANTS



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

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

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 SAFETY STANDARDS SERIES No. SSG-39

DESIGN OF INSTRUMENTATION AND CONTROL SYSTEMS FOR NUCLEAR POWER PLANTS

SPECIFIC SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

COPYRIGHT NOTICE

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

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

© IAEA, 2016

Printed by the IAEA in Austria

April 2016

STI/PUB/1694

IAEA Library Cataloguing in Publication Data

Design of instrumentation and control systems for nuclear power plants : specific safety guide. — Vienna : International Atomic Energy Agency, 2016.

p. ; 24 cm. — (IAEA safety standards series, ISSN 1020-525X ; no. SSG-39)

STI/PUB/1694

ISBN 978-92-0-102815-0

Includes bibliographical references.

1. Nuclear power plants — Design and construction — Safety measures.
2. Nuclear power plants — Instruments
3. Nuclear power plants — Control rooms. I. International Atomic Energy Agency. II. Series.

IAEAL

15-00999

FOREWORD

by Yukiya Amano
Director General

The IAEA's Statute authorizes the Agency to “establish or adopt... standards of safety for protection of health and minimization of danger to life and property” — standards that the IAEA must use in its own operations, and which States can apply by means of their regulatory provisions for nuclear and radiation safety. The IAEA does this in consultation with the competent organs of the United Nations and with the specialized agencies concerned. A comprehensive set of high quality standards under regular review is a key element of a stable and sustainable global safety regime, as is the IAEA's assistance in their application.

The IAEA commenced its safety standards programme in 1958. The emphasis placed on quality, fitness for purpose and continuous improvement has led to the widespread use of the IAEA standards throughout the world. The Safety Standards Series now includes unified Fundamental Safety Principles, which represent an international consensus on what must constitute a high level of protection and safety. With the strong support of the Commission on Safety Standards, the IAEA is working to promote the global acceptance and use of its standards.

Standards are only effective if they are properly applied in practice. The IAEA's safety services encompass design, siting and engineering safety, operational safety, radiation safety, safe transport of radioactive material and safe management of radioactive waste, as well as governmental organization, regulatory matters and safety culture in organizations. These safety services assist Member States in the application of the standards and enable valuable experience and insights to be shared.

Regulating safety is a national responsibility, and many States have decided to adopt the IAEA's standards for use in their national regulations. For parties to the various international safety conventions, IAEA standards provide a consistent, reliable means of ensuring the effective fulfilment of obligations under the conventions. The standards are also applied by regulatory bodies and operators around the world to enhance safety in nuclear power generation and in nuclear applications in medicine, industry, agriculture and research.

Safety is not an end in itself but a prerequisite for the purpose of the protection of people in all States and of the environment — now and in the future. The risks associated with ionizing radiation must be assessed and controlled without unduly limiting the contribution of nuclear energy to equitable and sustainable development. Governments, regulatory bodies and operators everywhere must ensure that nuclear material and radiation sources are used beneficially, safely and ethically. The IAEA safety standards are designed to facilitate this, and I encourage all Member States to make use of them.

THE IAEA SAFETY STANDARDS

BACKGROUND

Radioactivity is a natural phenomenon and natural sources of radiation are features of the environment. Radiation and radioactive substances have many beneficial applications, ranging from power generation to uses in medicine, industry and agriculture. The radiation risks to workers and the public and to the environment that may arise from these applications have to be assessed and, if necessary, controlled.

Activities such as the medical uses of radiation, the operation of nuclear installations, the production, transport and use of radioactive material, and the management of radioactive waste must therefore be subject to standards of safety.

Regulating safety is a national responsibility. However, radiation risks may transcend national borders, and international cooperation serves to promote and enhance safety globally by exchanging experience and by improving capabilities to control hazards, to prevent accidents, to respond to emergencies and to mitigate any harmful consequences.

States have an obligation of diligence and duty of care, and are expected to fulfil their national and international undertakings and obligations.

International safety standards provide support for States in meeting their obligations under general principles of international law, such as those relating to environmental protection. International safety standards also promote and assure confidence in safety and facilitate international commerce and trade.

A global nuclear safety regime is in place and is being continuously improved. IAEA safety standards, which support the implementation of binding international instruments and national safety infrastructures, are a cornerstone of this global regime. The IAEA safety standards constitute a useful tool for contracting parties to assess their performance under these international conventions.

THE IAEA SAFETY STANDARDS

The status of the IAEA safety standards derives from the IAEA's Statute, which authorizes the IAEA to establish or adopt, in consultation and, where appropriate, in collaboration with the competent organs of the United Nations and with the specialized agencies concerned, standards of safety for protection of health and minimization of danger to life and property, and to provide for their application.

With a view to ensuring the protection of people and the environment from harmful effects of ionizing radiation, the IAEA safety standards establish fundamental safety principles, requirements and measures to control the radiation exposure of people and the release of radioactive material to the environment, to restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation, and to mitigate the consequences of such events if they were to occur. The standards apply to facilities and activities that give rise to radiation risks, including nuclear installations, the use of radiation and radioactive sources, the transport of radioactive material and the management of radioactive waste.

Safety measures and security measures¹ have in common the aim of protecting human life and health and the environment. Safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.

The IAEA safety standards reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from harmful effects of ionizing radiation. They are issued in the IAEA Safety Standards Series, which has three categories (see Fig. 1).

Safety Fundamentals

Safety Fundamentals present the fundamental safety objective and principles of protection and safety, and provide the basis for the safety requirements.

Safety Requirements

An integrated and consistent set of Safety Requirements establishes the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements are governed by the objective and principles of the Safety Fundamentals. If the requirements are not met, measures must be taken to reach or restore the required level of safety. The format and style of the requirements facilitate their use for the establishment, in a harmonized manner, of a national regulatory framework. Requirements, including numbered ‘overarching’ requirements, are expressed as ‘shall’ statements. Many requirements are not addressed to a specific party, the implication being that the appropriate parties are responsible for fulfilling them.

¹ See also publications issued in the IAEA Nuclear Security Series.

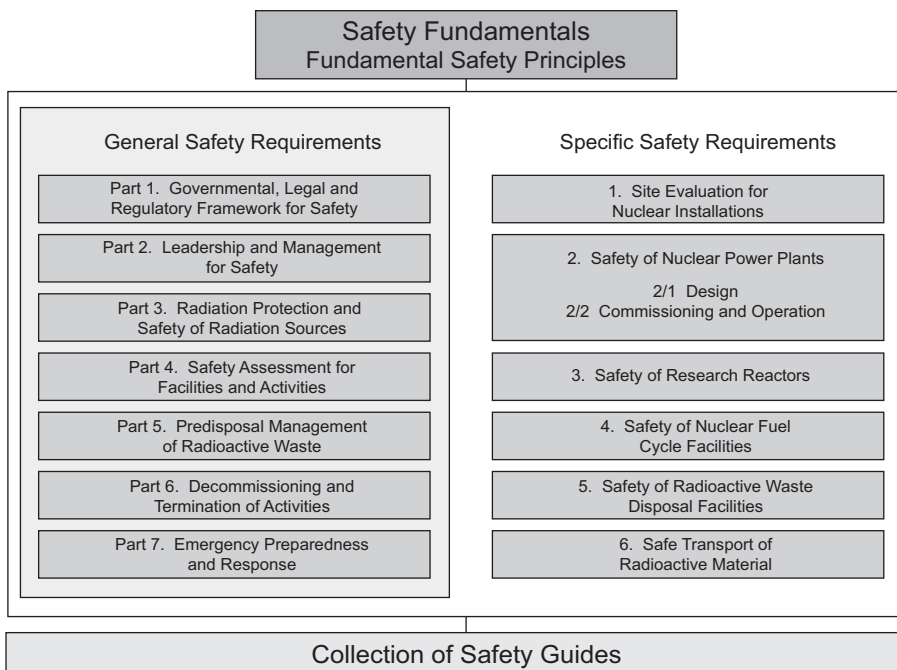


FIG. 1. The long term structure of the IAEA Safety Standards Series.

Safety Guides

Safety Guides provide recommendations and guidance on how to comply with the safety requirements, indicating an international consensus that it is necessary to take the measures recommended (or equivalent alternative measures). The Safety Guides present international good practices, and increasingly they reflect best practices, to help users striving to achieve high levels of safety. The recommendations provided in Safety Guides are expressed as ‘should’ statements.

APPLICATION OF THE IAEA SAFETY STANDARDS

The principal users of safety standards in IAEA Member States are regulatory bodies and other relevant national authorities. The IAEA safety standards are also used by co-sponsoring organizations and by many organizations that design, construct and operate nuclear facilities, as well as organizations involved in the use of radiation and radioactive sources.

The IAEA safety standards are applicable, as relevant, throughout the entire lifetime of all facilities and activities — existing and new — utilized for peaceful purposes and to protective actions to reduce existing radiation risks. They can be used by States as a reference for their national regulations in respect of facilities and activities.

The IAEA's Statute makes the safety standards binding on the IAEA in relation to its own operations and also on States in relation to IAEA assisted operations.

The IAEA safety standards also form the basis for the IAEA's safety review services, and they are used by the IAEA in support of competence building, including the development of educational curricula and training courses.

International conventions contain requirements similar to those in the IAEA safety standards and make them binding on contracting parties. The IAEA safety standards, supplemented by international conventions, industry standards and detailed national requirements, establish a consistent basis for protecting people and the environment. There will also be some special aspects of safety that need to be assessed at the national level. For example, many of the IAEA safety standards, in particular those addressing aspects of safety in planning or design, are intended to apply primarily to new facilities and activities. The requirements established in the IAEA safety standards might not be fully met at some existing facilities that were built to earlier standards. The way in which IAEA safety standards are to be applied to such facilities is a decision for individual States.

The scientific considerations underlying the IAEA safety standards provide an objective basis for decisions concerning safety; however, decision makers must also make informed judgements and must determine how best to balance the benefits of an action or an activity against the associated radiation risks and any other detrimental impacts to which it gives rise.

DEVELOPMENT PROCESS FOR THE IAEA SAFETY STANDARDS

The preparation and review of the safety standards involves the IAEA Secretariat and four safety standards committees, for nuclear safety (NUSSC), radiation safety (RASSC), the safety of radioactive waste (WASSC) and the safe transport of radioactive material (TRANSSC), and a Commission on Safety Standards (CSS) which oversees the IAEA safety standards programme (see Fig. 2).

All IAEA Member States may nominate experts for the safety standards committees and may provide comments on draft standards. The membership of the Commission on Safety Standards is appointed by the Director General and

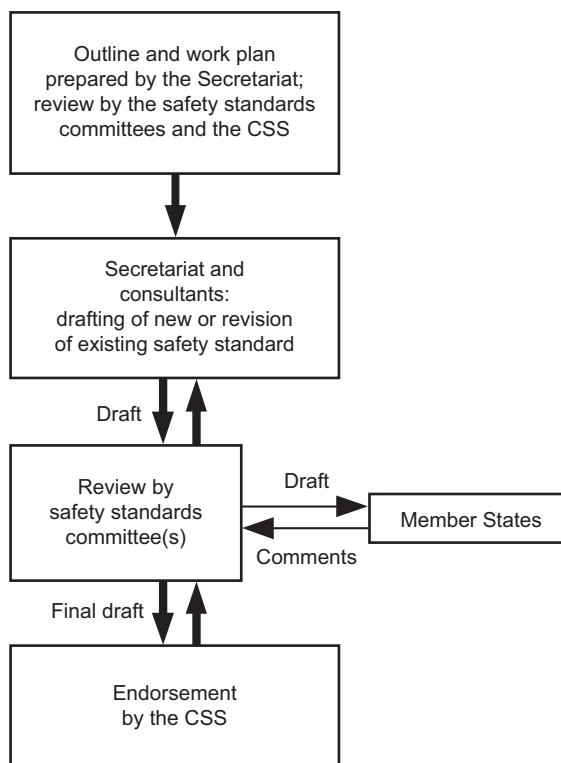


FIG. 2. The process for developing a new safety standard or revising an existing standard.

includes senior governmental officials having responsibility for establishing national standards.

A management system has been established for the processes of planning, developing, reviewing, revising and establishing the IAEA safety standards. It articulates the mandate of the IAEA, the vision for the future application of the safety standards, policies and strategies, and corresponding functions and responsibilities.

INTERACTION WITH OTHER INTERNATIONAL ORGANIZATIONS

The findings of the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) and the recommendations of international expert bodies, notably the International Commission on Radiological Protection (ICRP), are taken into account in developing the IAEA safety standards. Some

safety standards are developed in cooperation with other bodies in the United Nations system or other specialized agencies, including the Food and Agriculture Organization of the United Nations, the United Nations Environment Programme, the International Labour Organization, the OECD Nuclear Energy Agency, the Pan American Health Organization and the World Health Organization.

INTERPRETATION OF THE TEXT

Safety related terms are to be understood as defined in the IAEA Safety Glossary (see <http://www-ns.iaea.org/standards/safety-glossary.htm>). Otherwise, words are used with the spellings and meanings assigned to them in the latest edition of The Concise Oxford Dictionary. For Safety Guides, the English version of the text is the authoritative version.

The background and context of each standard in the IAEA Safety Standards Series and its objective, scope and structure are explained in Section 1, Introduction, of each publication.

Material for which there is no appropriate place in the body text (e.g. material that is subsidiary to or separate from the body text, is included in support of statements in the body text, or describes methods of calculation, procedures or limits and conditions) may be presented in appendices or annexes.

An appendix, if included, is considered to form an integral part of the safety standard. Material in an appendix has the same status as the body text, and the IAEA assumes authorship of it. Annexes and footnotes to the main text, if included, are used to provide practical examples or additional information or explanation. Annexes and footnotes are not integral parts of the main text. Annex material published by the IAEA is not necessarily issued under its authorship; material under other authorship may be presented in annexes to the safety standards. Extraneous material presented in annexes is excerpted and adapted as necessary to be generally useful.

CONTENTS

1.	INTRODUCTION	1
	Background (1.1–1.6)	1
	Objective (1.7–1.8)	3
	Scope (1.9–1.17)	3
	Structure (1.18–1.27)	5
2.	THE MANAGEMENT SYSTEM FOR INSTRUMENTATION AND CONTROL DESIGN	6
	General (2.1–2.9)	6
	Use of life cycle models (2.10–2.37)	9
	Activities common to all life cycle phases (2.38–2.91)	16
	Life cycle activities (2.92–2.167)	26
3.	DESIGN BASIS FOR INSTRUMENTATION AND CONTROL SYSTEMS	36
	Identification of instrumentation and control functions (3.1–3.6)	36
	Content of design basis for instrumentation and control systems (3.7–3.16)	37
4.	INSTRUMENTATION AND CONTROL ARCHITECTURE	41
	Architectural design (4.1–4.10)	41
	Content of the overall instrumentation and control architecture (4.11–4.12)	43
	Content of individual instrumentation and control system architectures (4.13)	44
	Independence (4.14–4.24)	44
	Consideration of common cause failure (4.25–4.40)	46
5.	SAFETY CLASSIFICATION OF INSTRUMENTATION AND CONTROL FUNCTIONS, SYSTEMS AND EQUIPMENT (5.1–5.13)	48

6.	GENERAL RECOMMENDATIONS FOR ALL INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY	50
	General (6.1–6.5)	50
	Design for reliability (6.6–6.76)	51
	Equipment qualification (6.77–6.134)	62
	Design to cope with ageing and obsolescence (6.135–6.152)	69
	Control of access to systems important to safety (6.153–6.158)	72
	Testing and testability during operation (6.159–6.191)	72
	Maintainability (6.192–6.197)	79
	Provisions for removal from service for testing or maintenance (6.198–6.204)	80
	Set points (6.205–6.212)	81
	Marking and identification of items important to safety (6.213–6.219)	82
7.	DESIGN GUIDELINES FOR SPECIFIC INSTRUMENTATION AND CONTROL SYSTEMS, AND EQUIPMENT	84
	Sensing devices (7.1–7.9)	84
	Control systems (7.10–7.14)	85
	Protection system (7.15–7.59)	86
	Power supplies (7.60–7.65)	92
	Digital systems (7.66–7.147)	93
	Software tools (7.148–7.164)	103
	Qualification of industrial digital devices of limited functionality for safety applications (7.165–7.175)	106
8.	CONSIDERATIONS RELATING TO THE HUMAN–MACHINE INTERFACE	108
	Control rooms (8.1–8.18)	108
	Accident monitoring (8.19–8.35)	111
	Operator communications systems (8.36–8.46)	113
	General principles relating to human factors engineering for instrumentation and control systems (8.47–8.93)	115
	Recording of historical data (8.94)	121

9.	SOFTWARE	121
	General (9.1–9.5)	121
	Software requirements (9.6–9.15)	122
	Software design (9.16–9.43)	124
	Software implementation (9.44–9.63)	127
	Software verification and analysis (9.64–9.95)	129
	Predeveloped software (9.96–9.98)	132
	Software tools (9.99)	133
	Third party assessment (9.100–9.103)	133
	REFERENCES	135
ANNEX I:	BIBLIOGRAPHY OF INTERNATIONAL INSTRUMENTATION AND CONTROL STANDARDS ..	139
ANNEX II:	CORRELATION BETWEEN THIS SAFETY GUIDE AND IAEA SAFETY STANDARDS SERIES Nos NS-G-1.1 AND NS-G-1.3	146
ANNEX III:	AREAS WHERE PRACTICES OF MEMBER STATES DIFFER	150
	DEFINITIONS	155
	CONTRIBUTORS TO DRAFTING AND REVIEW	159

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide provides recommendations on the design of instrumentation and control (I&C) systems to meet the requirements established in IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [1].

1.2. This publication is a revision and combination of two Safety Guides, namely IAEA Safety Standards Series Nos NS-G-1.1¹ and NS-G-1.3², which it supersedes. The revision takes into account developments in I&C systems since the publication of these earlier Safety Guides in 2000 and 2002, respectively. The main changes relate to the continuing development of computer applications and the evolution of the methods necessary for their safe, secure and practical use. In addition, account is taken of developments in human factors engineering and the need for computer security. This Safety Guide references and takes into account other IAEA Safety Standards and Nuclear Security Series publications that provide guidance relating to I&C design. Most notable among these are the IAEA Safety Standards Series Nos GS-R-3, The Management System for Facilities and Activities [2], GS-G-3.1, Application of the Management System for Facilities and Activities [3], GS-G-3.5, The Management System for Nuclear Installations [4], and GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities [5].

1.3. The main topical areas for which this Safety Guide provides new or updated guidance are the following:

- Considerations specific to I&C for achieving compliance with the requirements established in GS-R-3 [2];
- Design inputs to be considered when developing the design basis for I&C systems;

¹ INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

² INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).

- The interdependent nature of life cycles for the design and implementation of I&C systems, and in particular the life cycle for the overall I&C for the facility as a whole, for individual I&C systems and for software, and the need for integration of human factors engineering inputs and computer security inputs into those life cycles;
- The use of computers, devices programmed with hardware description languages and industrial devices of limited functionality, and means of gaining assurance of their correct performance;
- The overall I&C architecture in support of the concept of defence in depth applied in the design of the plant systems and in establishing defence in depth for the I&C system itself as protection against common cause failure;
- Data transport between systems important to safety, with special consideration for cases where the system receiving data is in a higher safety class than the system sending data;
- Provisions for ensuring the security of digital safety systems;
- Activities relating to the development of computer software, including design, verification and validation, derived from principles given in this Safety Guide or implicit in the previous Safety Guide, NS-G-1.1³.

1.4. Throughout this Safety Guide, the term ‘I&C system’ refers to any I&C system important to safety as defined by the IAEA Safety Glossary [6]. The term ‘important to safety’ is not repeated again except for emphasis. In cases where recommendations or explanations are applicable to both I&C systems important to safety and I&C systems that are not important to safety, this is explicitly stated.

1.5. This Safety Guide is closely related to IAEA Safety Standards Series No. SSG-34, Design of Electrical Power Systems for Nuclear Power Plants [7], which provides recommendations for power supply, cable systems, protection against electromagnetic interference, equipment and signal grounds, and other topics that are necessary for the satisfactory operation of I&C systems.

1.6. Additional guidance on the design and development of I&C systems, equipment and software is available from States and from other organizations that develop standards. Such publications give much greater detail than is appropriate for IAEA safety standards. It is expected that this Safety Guide will be used in conjunction with detailed industrial standards.

³ See footnote 1.

OBJECTIVE

1.7. The objective of this Safety Guide is to provide guidance on the overall I&C architecture and on the I&C systems important to safety in nuclear power plants for meeting the safety goals of the plant.

1.8. This Safety Guide identifies the input information needed by I&C designers to define the I&C design basis from the mechanical, electrical, nuclear and civil engineering design of the plant, from the plant layout process and from safety analysis. The I&C design basis will, for example, provide the functional requirements to be achieved by the I&C, the extremes of environmental temperature in which equipment is required to operate, the external events that I&C equipment is required to withstand, and the conditions for which an automatic shutdown is required to take place.

SCOPE

1.9. This Safety Guide provides guidance on the design, implementation, qualification and documentation of I&C systems important to safety in nuclear power plants to meet the requirements of SSR-2/1 (Rev. 1) [1]. This Safety Guide also describes certain I&C specific issues that are relevant to implementing the recommendations of certain other Safety Guides, such as those that cover the management system, commissioning, installation, operation, and operating limits and conditions. For such cases, this Safety Guide identifies relevant sections of these other Safety Guides.

1.10. The guidance applies to all I&C equipment, from sensors to the devices that actuate and control mechanical equipment. It covers, for example:

- Sensors;
- Actuator controls;
- Equipment for automatic and manual control of plant equipment;
- Operator interfaces.

1.11. This Safety Guide also applies to the means for implementing I&C equipment, such as:

- Computer systems and associated communication systems;
- Software;

- Devices that are programmed using hardware description languages (e.g. field programmable gate arrays);
- Industrial digital devices of limited functionality.

1.12. This Safety Guide does not provide recommendations for support features for I&C systems, such as cooling, lubrication and energy supply. Recommendations for electrical power supply are provided in SSG-34 [7].⁴

1.13. Although this Safety Guide covers certain aspects of human factors and computer security as they relate to I&C, it does not provide comprehensive guidance on these domains. The intent in this Safety Guide is to identify major interfaces with the human factors and computer security activities, and to give recommendations on I&C design features that affect these topics. Examples of human factors and computer security topics not covered in this guide include computerized operating procedures and information technology security. More detailed information on computer security is provided in Ref. [8].

1.14. The guidance applies to the design of I&C systems for new plants, to modifications of existing plants and to the modernization of the I&C of existing plants. IAEA Safety Standards Series No. NS-G-2.3, Modifications to Nuclear Power Plants [9] deals with plant modification, and the overlap of this Safety Guide with NS-G-2.3 [9] has been kept to a minimum.

1.15. The IAEA Safety Glossary [6] defines I&C systems important to safety as those I&C systems that are part of a safety group and also those I&C systems whose malfunction or failure could lead to radiation exposure of site personnel or members of the public. Section 5 of this Safety Guide further discusses the term ‘important to safety’ and other terminology relating to safety classification. Examples of I&C systems to which this Safety Guide may apply include:

- Reactor protection systems;
- Reactor control systems and reactivity control systems and their monitoring systems;
- Systems for monitoring and controlling reactor cooling;
- Systems for monitoring and controlling emergency power supplies;
- Systems for monitoring and controlling containment isolation;
- Instrumentation for accident monitoring;

⁴ A draft Safety Guide on the topic of auxiliary systems that will provide recommendations for other support features is currently under development.

- Systems for monitoring of effluents;
- I&C systems for fuel handling.

1.16. This Safety Guide provides recommendations for the development of computer software for use in I&C systems important to safety as well as for digital data communication. This Safety Guide also defines measures needed for I&C functions that are programmed into integrated circuits using hardware description language.

1.17. References [10, 11] present overviews of concepts that underlie this Safety Guide and give examples of systems addressed in it. These references may provide useful background material for some users, although they do not provide IAEA guidance.

STRUCTURE

1.18. Section 2 provides guidance for the application of the requirements in GS-R-3 [2] and the recommendations of GS-G-3.1 [3] and GS-G-3.5 [4] as they relate specifically to the development of I&C systems. It also addresses the use of life cycle models to describe management system processes for the development of I&C, provides guidance on generic processes for I&C design and provides guidance on the conduct of specific I&C development activities.

1.19. Section 3 identifies the necessary inputs to the design and provides recommendations on the design basis for I&C systems.

1.20. Section 4 provides guidance on the architecture of the overall I&C for the plant.

1.21. Section 5 describes the safety classification scheme that is used to grade the application of the recommendations of this Safety Guide in accordance with the safety significance of items to which they apply.

1.22. Section 6 provides general guidance applicable to all I&C systems important to safety.

1.23. Section 7 provides recommendations that are specific to certain systems such as the reactor protection system, certain types of equipment such as sensors, and certain technologies such as digital systems and integrated circuits configured

with hardware description languages. The recommendations of Sections 2–6 and Sections 8 and 9 also apply to the specific systems discussed in Section 7.

1.24. Section 8 provides recommendations on the human–machine interface. It includes guidance on the application of human factors principles to I&C and the characteristics that the human–machine interface should have.

1.25. Section 9 provides guidance on the development of software for computer based I&C systems important to safety.

1.26. This Safety Guide should be applied as a whole, not as a series of stand-alone sections. For example, the guidance on software provided in Section 9 is to be applied in conjunction with the guidance on the management system and on life cycles given in Section 2.

1.27. The annexes include a listing of industrial standards that provide more detailed guidance on the topical areas of this Safety Guide, information relating this Safety Guide to the two Safety Guides (NS-G-1.1⁵ and NS-G-1.3⁶) it supersedes, and a summary of areas where practices of States differ. A list of definitions specific to this Safety Guide is also provided.

2. THE MANAGEMENT SYSTEM FOR INSTRUMENTATION AND CONTROL DESIGN

GENERAL

2.1. Requirement 6 of SSR-2/1 (Rev. 1) [1] states that:

“The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.”

⁵ See footnote 1.

⁶ See footnote 2.

2.2. Requirement 2 of SSR-2/1 (Rev. 1) [1] states that:

“The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design.”

2.3. GS-R-3 [2] establishes requirements for the management system for facilities and activities.

2.4. Paragraph 2.1 of GS-R-3 [2] states that:

“A management system shall be established, implemented, assessed and continually improved. It shall be aligned with the goals of the organization and shall contribute to their achievement. The main aim of the management system shall be to achieve and enhance safety by:

- Bringing together in a coherent manner all the requirements for managing the organization;
- Describing the planned and systematic actions necessary to provide adequate confidence that all these requirements are satisfied;
- Ensuring that health, environmental, security, quality and economic requirements are not considered separately from safety requirements, to help preclude their possible negative impact on safety.”

Paragraph 4.2 of GS-R-3 [2] further states: “The information and knowledge of the organization shall be managed as a resource.”

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

2.6. The management system includes the organizational structure, the organizational culture, policies and processes, including those to identify and allocate resources (e.g. personnel, equipment, infrastructure and the working environment) for developing I&C systems that meet safety requirements.

2.7. Each organization involved in I&C development activities should have a management system that is consistent with the expectations of the management system of the operating organization.

2.8. GS-G-3.1 [3] and GS-G-3.5 [4] provide guidance on the application of the requirements established in GS-R-3 [2] for facilities and activities, and for nuclear installations.

2.9. The management system for the development of I&C systems should meet the requirements of GS-R-3 [2] and be in accordance with the recommendations provided in GS-G-3.1 [3] and GS-G-3.5 [4], which apply broadly for the development of all structures, systems and components in a nuclear power plant. This Safety Guide, which addresses the specific development processes needed for I&C systems, should be used in conjunction with these publications.

The topics of GS-R-3 [2] that are of particular interest in the development of I&C systems are:

- The management system;
- Safety culture;
- Management commitment;
- Compliance with statutory and regulatory requirements;
- Organizational policies;
- Planning;
- Responsibilities and authority;
- Provision of resources;
- Human resources;
- Development of management system processes;
- Process management;
- Control of documents, products (including tools) and records;
- Purchasing;
- Communication;
- Management of organizational change;
- Monitoring and measurement;
- Self-assessment;
- Independent assessment;

- Non-conformances and corrective and preventative actions;
- Improvement.

USE OF LIFE CYCLE MODELS

2.10. Paragraph 5.1 of GS-R-3 [2] states:

“The processes of the management system that are needed to achieve the goals, provide the means to meet all requirements and deliver the products of the organization shall be identified, and their development shall be planned, implemented, assessed and continually improved.”

2.11. Modern I&C systems in nuclear power plants are complex entities for which different approaches to design and qualification are necessary beyond those that were typically applied to older systems. Frequently, the functional characteristics and performance of previous generations of I&C systems were characterized by models based on physics principles and testing that validated these models.

2.12. Modern I&C systems, in particular digital systems whose functionality depends on software or a hardware definition language, are fundamentally different from older systems in that their behaviour is determined by logic and is not prescribed by external physical laws. Consequently, minor errors in design and implementation can cause digital systems to exhibit unexpected behaviour.

2.13. In digital I&C systems, demonstration that the final product is fit for its purpose depends greatly, but not exclusively, on the use of a high quality development process that provides for disciplined specification and implementation of design requirements. Verification and validation activities are necessary for ensuring that the final product is suitable for use. However, correct performance of digital I&C systems over the full range of conditions cannot be inferred from a combination of testing and physics models to the same extent that this can be done for systems that rely only on hardware. Consequently, confidence in the correctness of modern systems derives more from the discipline of the development process than was the case for systems implemented purely with hardware.

2.14. In response to this situation, in the nuclear power domain as well as in other safety-critical domains such as aerospace, development processes have been applied that are commonly represented as life cycle models, which describe the

activities for the development of electronic systems and the relationships between these activities. These commonly accepted practices have been formalized in nuclear standards that provide extensive guidance regarding processes for developing I&C systems. Normally, activities relating to a given development step are grouped into the same phase of the life cycle.

2.15. A well documented development process will also produce evidence that can allow independent reviewers and the regulatory body to gain confidence in the fitness for purpose of the final product.

2.16. The recommendations for life cycle processes provided in this section also apply to the life cycle activities described in Section 9. The guidance on life cycle processes in this section supplements the requirements of GS-R-3 [2] and the recommendations of GS-G-3.1 [3] and GS-G-3.5 [4] as they apply to the development of I&C systems.

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

- (a) An overall I&C architecture life cycle;
- (b) One or more individual I&C system life cycles;
- (c) One or more individual component life cycles: Component life cycles are typically managed in the framework of platform development and are independent of the overall architecture level and the individual system level life cycles. Component life cycles for digital systems are typically divided into separate life cycles for the development of hardware and software.

2.18. Other activities sometimes outside of the development of I&C systems will have an important influence on the requirements for, and the design of, I&C systems. Human factors engineering and computer security are examples of such activities. Such activities have a broader purpose than the support of I&C system design, but they will have a strong influence on I&C development. Furthermore, it is easier and more cost efficient to take account of human factors and security features in the design phase. After the design phase, changes can be very difficult or even impossible to implement.

2.19. Figure 1 shows an example of an I&C development life cycle and the main inputs received from the human factors engineering and computer security programmes.

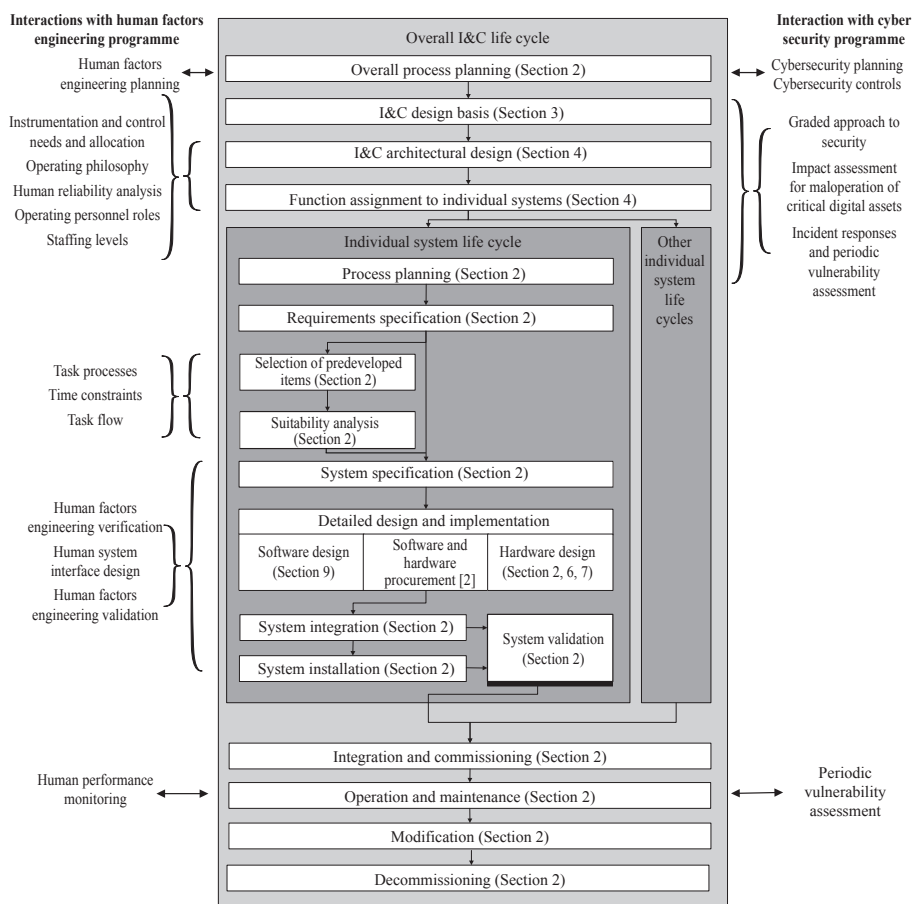


FIG. 1. Typical I&C development life cycle activities and interfaces with human factors engineering and computer security programmes.

2.20. The ‘V-model’ shown in Fig. 2 is a useful alternative view of a sample development life cycle. This model illustrates the relationship between requirements specification, design, integration and system validation, and how verification and validation activities relate to development activities. Figure 2 applies to both digital and analogue systems. Of course, if there is no software, the software activities are unnecessary.

2.21. At any point in the life cycle, experience gained might result in a need to revise work done in a previous phase. These changes will then flow through and affect work from the intervening phases. For simplicity, Figs 1 and 2 do not show such iteration paths.

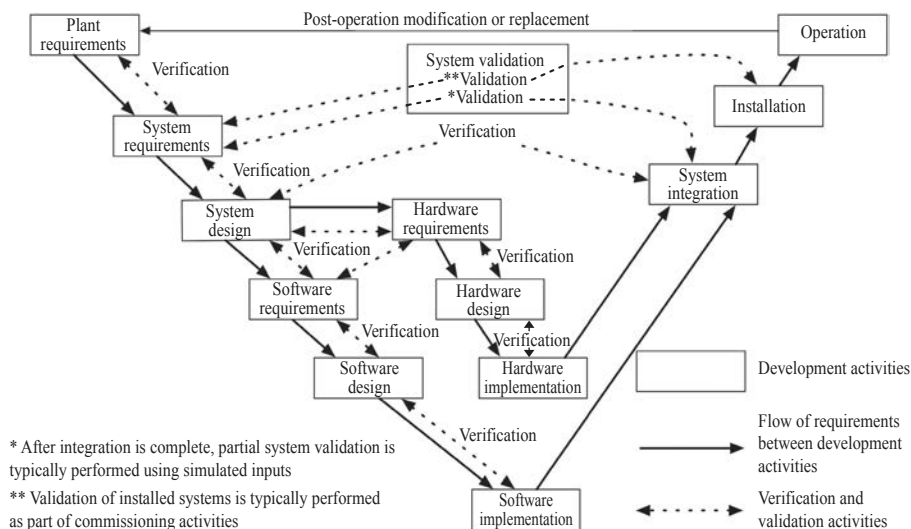


FIG. 2. Typical relationship between I&C development life cycle processes and verification and validation activities.

2.22. All activities associated with development, implementation and operation of the overall I&C architecture, individual I&C systems and I&C components⁷ should be carried out in the framework of a documented development life cycle.

2.23. The life cycle of each I&C system and component should cover a period that starts with the derivation of its requirements and ends when the I&C system or component is no longer required for the safety of the plant.

Process planning

2.24. Before the initiation of any technical activity, a plan identifying the necessary inputs and the products and processes of that activity, and the relationship of the activity with other activities, should be prepared and approved in accordance with the requirements for the management system.

2.25. Plans for the development of I&C systems deal with topics that are specific to I&C and with topics for which I&C development may need specialized

⁷ I&C components include hardware, software, such as application software and firmware, and hardware description language.

treatment. Typically, plans specific to I&C development will be prepared to deal with the topics given in the following:

- Life cycle models;
- Configuration management;
- Identification, control and resolution of non-conformances;
- Hazard analysis;
- Verification and validation;
- Use of insights from probabilistic safety assessment;
- Safety analysis specific to I&C systems;
- Requirements engineering;
- Architectural design;
- Selection and acceptance of predeveloped items;
- Design;
- Implementation (e.g. hardware manufacture and coding of software or coding and synthesis using a hardware description language);
- Integration;
- System validation;
- Installation;
- Commissioning;
- Equipment qualification;
- Qualification and use of tools;
- Maintainability;
- Mitigation of obsolescence;
- Operation;
- Training;
- Software maintenance.

2.26. The plans for several of these topics may be combined into a single plan.

2.27. The development of I&C systems also depends on plans for activities that are not specific to I&C development, such as:

- Quality assurance;
- Classification of items important to safety;
- Purchasing;
- Manufacturing;
- Production and maintenance of documentation.

2.28. All I&C development activities should be performed in accordance with the applicable approved plans.

Coordination with human factors engineering activities and computer security activities

2.29. Although life cycle models relating to human factors engineering and computer security are not covered by this Safety Guide, such processes provide information that is required for I&C development. Figure 1 illustrates the relationships and interfaces between these processes. These include: activities that produce requirements specific to human factors engineering; outputs of verification and validation activities relating to human factors engineering; technical security measures; and computer security requirements.

2.30. The development of I&C systems should be coordinated with human factors engineering activities and computer security activities.

2.31. In the development of I&C systems, requirements arising out of the human factors engineering programme should be taken into account, including:

- The specification of roles and responsibilities of operating personnel and other staffing requirements;
- Safety classification of the structures, systems and components of the human-machine interface;
- The specification of information needs, including considerations for defining a subset of indications and controls required to address accident conditions and post-accident conditions;
- The specification of control needs, automatic and manual control functionality, and the allocation of controls to suitable locations;
- Requirements relating to task processes, time constraints and the flow of operating personnel and information as identified by analyses (i.e. task analysis; see para. 8.78);
- Strategies for context based annunciation; context based annunciation avoids ‘flooding’ of messages, for example, during startup and during transients;
- Requirements for the reporting of I&C system faults;
- Provisions in support of I&C maintainability;
- Insights resulting from the consideration of the potential for human error in safety analysis (i.e. human reliability analysis).

2.32. Verification and validation activities relating to human factors engineering:

- Should verify the resolution of recommendations relating to human factors engineering and deficiencies identified during analyses of the design of the human-machine interface;
- Should verify that the I&C systems conform to applicable design guidelines relating to human factors engineering;
- Should verify that the design provides I&C systems, other equipment and operator aids that are adequate for supporting operating personnel in the performance of their assigned tasks;
- Should verify that the human factors design elicits proper operator response to annunciation messages, including allowing adequate time for credited operator actions;
- Should validate, using performance based measures, that operating personnel can carry out their functions using the I&C system under all conditions in which the system is expected to function, including when some parts of the I&C system are out of service for authorized reasons, for example, for purposes of maintenance or testing.

2.33. The development of human factors engineering requirements and the verification and validation of human factors engineering activities are normally performed as part of the human factors engineering programme. The human factors engineering programme is not described in any further detail within this Safety Guide, with the exception of interfaces to the I&C life cycle process.

2.34. The overall I&C for the plant should implement the security measures that are assigned to it by the computer security plan.

2.35. The computer security plan should be updated, as necessary, to take into account the overall I&C architecture and individual I&C systems.

2.36. Development of I&C should be conducted through dialogue between personnel responsible for safety and for nuclear security or by a mixed team of safety and nuclear security personnel in a development environment that meets the technical, procedural and administrative requirements of the computer security plan.

2.37. Additional information on the implementation of computer security at nuclear facilities is provided in Ref. [8].

ACTIVITIES COMMON TO ALL LIFE CYCLE PHASES

Configuration management

2.38. Paragraphs 5.12, 5.13, 5.18 and 5.19 of GS-R-3 [2] state:

“5.12. Documents...shall be controlled...It shall be ensured that document users are aware of and use appropriate and correct documents.

“5.13. Changes to documents shall be reviewed and recorded and shall be subject to the same level of approval as the documents themselves.

.....

“5.18. Controls shall be used to ensure that products do not bypass the required verification activities.

“5.19. Products shall be identified to ensure their proper use. Where traceability is a requirement, the organization shall control and record the unique identification of the product.”

2.39. In GS-R-3 [2], these topics are addressed under the heading of control of documents, control of products and control of records. For engineering activities, the control of documents and of products is more commonly grouped under the heading of configuration management. The requirements of GS-R-3 [2] for control of records also apply to documents under configuration management, although some records may be controlled separately from the configuration management systems (e.g. by a separate records management system). GS-G-3.1 [3] and GS-G-3.5 [4] provide additional recommendations on the four topics indicated in para. 2.38.

2.40. The objectives of configuration management during the life cycle for I&C systems include:

- Identification of all items for which configuration management is required, i.e. documents, I&C products and associated records;
- Provision for secure storage and retrieval of configuration items;
- Identification of dependencies and relationships between items under configuration management;
- Identification of all changes of items under configuration management;

- Prevention of the inadvertent and unauthorized modification of items under configuration management;
- Ensuring continued conformance with the design basis;
- Specification of baselines for configuration, i.e. the configuration of mutually compatible and consistent components for an item at every hierarchical level of configuration under configuration management;⁸
- Ensuring consistency between the physical plant and the technical documentation;
- Specification of the current status of items under configuration management (e.g. their review or approval, or validation status).

2.41. Configuration management should include techniques and procedures for analysing the effects of changes, approving changes, ensuring versions are combined correctly, releasing design documents and software for use, and establishing and maintaining a chronological record (e.g. what versions of tools are to be used at a particular point in design).

2.42. All I&C items and their associated documents should be designated, given a unique identifier and placed under configuration management.

2.43. I&C items include the delivered I&C system, any separately installed items that support the system or are necessary for the system to operate as intended, the documents and files that define all of these items, and the software tools that might affect their quality.

2.44. I&C items typically include, for example:

- Procured items, reused items and newly developed items;
- Software components, such as source code and executable code, hardware description language, field programmable gate array configuration data (known as ‘bit stream’) and software that is installed in plant equipment, including applications software, operating systems and support software;
- Hardware components and replaceable elements of such components;
- Firmware;

⁸ Items for which a configuration baseline is established may include individual components, systems or the overall I&C system. The baseline for any item will cover all of the systems and components that comprise the item.

- Development documents such as specifications, design documents, fabrication drawings and instructions, installation drawings and instructions, software and hardware description language;
- Equipment configuration data and configuration files (e.g. safe operating limits, warning or alert limits, set points and calibration constants);
- Physical tools and software tools that are used to produce, control, configure, verify or validate I&C components, including the parameter settings used when employing such tools.

2.45. Configuration management data should be used to verify that I&C items are assembled correctly and installed in the correct physical and topological location, and that the intended software version is installed correctly.

2.46. Paragraph 5.21 of GS-R-3 [2] states that: “Records shall be specified in the process documentation and shall be controlled. All records shall be readable, complete, identifiable and easily retrievable.”

2.47. Life cycle process records should be placed under configuration management.

2.48. The configuration management programme for life cycle records may be different from that used for I&C products.

2.49. Life cycle records to be placed under configuration control include any information on which the system safety analysis depends or which could affect safety during operation or maintenance, for example:

- Plans and procedures for life cycle activities;
- The safety demonstration plan;
- Analysis documents;
- Artefacts or records that document the safety demonstration and its supporting evidence, for example, artefacts or records of assurance, verification (including analysis and testing), validation (including validation of requirements), process assessment and audit, authenticity, integrity and traceability;
- Records of verification and validation activities;
- Test specifications, procedures, plans and results;
- Limiting settings of safety systems and the methodology for establishing limiting settings of safety systems;
- Procedures, plans and results relating to system integration;
- Documents relating to review and audit of processes;

- Matrices providing traceability of requirements;
- Maintenance and operating procedures;
- Technical aspects of purchasing specifications for equipment and spares;
- Qualification records;
- Documentation of I&C systems and components (see para. 2.90).

2.50. The identification of items under configuration management should include the revision number.

2.51. Configuration control should be applied to the initial development of I&C systems, changes made during development and modifications after they have been placed in service.

2.52. The configuration management process should maintain relevant information for each item under configuration management.

2.53. Information that might be recorded includes: when the item was first considered to be complete; what changes were incorporated in the various versions including difference reports where appropriate; the dependencies on other items under configuration management; the item's current approval status; and the persons responsible for creating, reviewing and approving it.

2.54. The identity of software installed in I&C equipment and the values of configuration data should be retrievable from the I&C equipment itself.

2.55. The ability to retrieve the identity of installed items and the values of configuration data will support verification that the devices are properly configured. The installation of automatic checking features or software tools may assist in this verification.

Hazard analysis for instrumentation and control systems

2.56. For the overall I&C architecture, a hazard analysis should be performed to identify conditions that might compromise the defence in depth or the strategy for diversity of the plant design.

2.57. For each safety system, a hazard analysis should be performed to identify conditions that might degrade the performance of its safety function.

2.58. Hazards that should be considered include internal hazards and external hazards, failures of plant equipment and I&C failures or spurious operation due to hardware failure or software errors. Contributory hazards due to unwanted interactions should also be considered.

2.59. The hazard analysis for I&C systems should consider all plant states and operating modes, including transitions between different operating modes. Degraded states should also be included.

2.60. The initial results of the I&C system hazard analysis should be available before the design basis for the overall I&C is completed.

2.61. The hazard analysis should be updated at every phase of the development life cycle, including (but not limited to) the design of the overall I&C architecture, and the specification of requirements for and the design, implementation, installation and modification of safety systems.

2.62. The intent of updating the hazard analysis is to identify hazards that may be caused by specific characteristics of I&C safety systems, by interaction between I&C safety systems and the plant, and by interaction of I&C safety systems with other I&C systems, irrespective of their safety classification.

2.63. Measures should be taken to eliminate, avoid or mitigate the consequences of identified hazards that could degrade the performance of system functions.

2.64. Measures to eliminate, avoid or mitigate the consequences of hazards might, for example, take the form of changes to the requirements, design or implementation of I&C systems, or changes to the plant design.

2.65. The methods selected for hazard analysis should be appropriate for the item being analysed.

Verification and validation

2.66. Each phase of the life cycle for an I&C system uses information developed in earlier phases, and provides results to be used as the input for later phases.

2.67. The results of each phase in the life cycle should be verified against the requirements set by the previous phases.

2.68. A requirements traceability matrix can be used to document confirmation that requirements are satisfactorily met in each phase of the life cycle or that appropriate action was taken where requirements were not satisfactorily met.

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

2.70. Verification and validation should be carried out by individuals, teams or organizational groups that are independent of the designers and developers.

2.71. Establishment of the independence of verification and validation normally involves ensuring that the teams, individuals or organizational groups carrying out verification and validation:

- Have adequate technical competence and knowledge;
- Can set their own scope;
- Are not subject to pressure from the developers;
- Are not subject to reductions in budget or to constraints in schedules that would prevent them from completing the full scope of their review;
- Are allowed to submit their findings to management without adverse pressure from the development group.

2.72. The extent and type of independence of the verification and validation should be suitable for the safety class of the system or component involved. Verification and validation may occur in parallel at different levels of independence (e.g. verification and validation carried out by testers independent of developers in the original development organization, and additional independent verification and validation carried out by a separate organization).

2.73. Verification and validation activities, including records of detected anomalies and their disposition, should be documented. If anomalies are detected at the verification and validation stage, the resulting design modifications and their implementation should be subject to the same verification and validation process performed previously.

2.74. Technical communications between the verification and validation teams, system integration teams, commissioning teams, and the system designers and developers should be documented.

Use of insights from probabilistic safety analysis

2.75. Paragraph 5.76 of SSR-2/1 (Rev. 1) [1] states:

“The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to:

- (a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;
- (b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; [footnote omitted]
- (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.”

2.76. Insights gained from probabilistic safety assessment should be considered in the design of I&C systems.

2.77. Detailed information on probabilistic safety assessment and the use of results from probabilistic safety assessment during design can be found in the relevant IAEA Safety Standards [12, 13].

Safety assessment

2.78. Safety assessment of I&C should be conducted in accordance with the requirements of GSR Part 4 (Rev. 1) [5] and the recommendations of IAEA Safety Standards Series Nos SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [12] and SSG-2, Deterministic Safety Analysis for Nuclear Power Plants [14].

2.79. Design analyses and verification and validation should be performed to confirm that all design basis requirements of the overall I&C architecture and each individual I&C system are met.

2.80. Paragraph 3.14 recommends topics to be considered in the design basis requirements for the overall I&C architecture and all I&C systems. Paragraph 3.15 recommends additional topics to be considered in the design basis requirements for safety systems.

2.81. Typical design analysis, verification and validation techniques include:

- Traceability analysis: Traceability analysis is typically used to confirm implementation and validation of requirements.
- Failure mode and effects analysis: Failure mode and effects analysis is often used to confirm compliance with the single failure criterion and to confirm that all known failure modes are either self-revealing or detectable by planned testing.
- Analysis of defence in depth and diversity: Analysis of defence in depth and diversity is one of the means of investigating the vulnerability of safety systems to common cause failure (see Ref. [11], which provides additional information on this topic).
- Reliability analysis: Reliability analysis uses statistical methods to predict the reliability of systems or components. Commonly used reliability analysis techniques include parts count analysis, parts stress analysis, life data analysis (e.g. Weibull analysis), reliability block diagrams and fault tree analysis.
- Validation: Validation testing involves deterministic techniques and may include statistical techniques.
- Security testing: Security testing usually requires input from a vulnerability assessment and is used to confirm the use of good practice in security.
- Analysis to confirm that items have been designed for reliability: Such analysis is used to confirm that a design incorporates features that are known to promote high reliability, such as redundancy, compliance with the single failure criterion, testability, fail-safe design and rigorous qualification.⁹
- Confirmation of functional requirements for various operating modes of the I&C system: This includes analysis of correct system behaviour during and after power interruptions, restart or reboot, and other transition points. Calendar time changes (e.g. daylight saving time and leap years) are examples of other transition points.

⁹ For I&C systems, a combination of qualitative analysis, quantitative analysis and testing is usually needed to verify compliance with reliability requirements.

2.82. Each assumption used in an analysis should be stated and use of the assumption should be justified.

2.83. The methodology for any analysis conducted should be thoroughly defined and documented together with inputs into the analysis, results from the analysis and the analysis itself.

2.84. Given the current state of the art for an individual system that is specified and designed in accordance with the highest quality criteria, a figure of the order of 10^{-4} to 10^{-5} failure/demand may be an appropriate overall limit to place on the reliability that may be claimed in the probabilistic safety analysis, when all of the potential sources of failure (excluding cybersecurity related sources of failure) associated with the specification, design, manufacture, installation, operating environment and maintenance practices are taken into account. This figure may need to include the risk of common mode failure in the redundant channels of the system, and applies to the whole of the system, from sensors, through processing to the outputs, to the actuated equipment. Claims for better reliabilities than this are not precluded but will need special justification with account taken of all of the factors mentioned.

2.85. Any reliability claims for I&C systems should be substantiated and should be within justifiable limits (Annex III describes limits accepted in some States).

2.86. During the design and implementation process, the interaction of each I&C system with the plant should be reviewed regularly against the plant safety requirements and against the requirements of SSR-2/1 (Rev. 1) [1].

2.87. Where any conflict with these requirements is found, the design and implementation should be corrected appropriately.

Documentation

2.88. I&C documentation:

- Should provide a means of communicating information between the various phases of, and the various parties involved in, the design process;
- Should provide a record showing that all of the requirements have been correctly interpreted and fulfilled in the installed system;
- Should communicate operationally essential information and safety design related information to the plant operating personnel;

- Should provide a foundation for maintenance of the plant and I&C systems, and for potential future revisions to the design;
- Should be traceable throughout the I&C life cycle phases;
- Should be controlled under a configuration management system;
- Should be unambiguous, complete, consistent, well structured, readable, understandable to the target audience (e.g. domain experts, safety engineers and software designers), verifiable and maintainable.

2.89. Adequate documentation will facilitate operation, surveillance, troubleshooting, maintenance, future modification or modernization of the system, as well as training of plant and technical support staff.

2.90. The operating organization should establish or be provided with documentation for I&C systems and components that, as a minimum, cover the following topics:

- Design requirements;
- Functions and functional design;
- Principles of operation;
- The role of the system in the overall plant concept;
- Design features, including identification of features that are important to safety;
- As-built design and configuration documentation;
- As-built location of systems and their main components, including sensors and actuators;
- Interfaces with, and dependencies on, other plant systems;
- Facilities and requirements for surveillance, testing, diagnostics, maintenance and operation;
- Test procedures and results;
- Equipment qualification;
- The design and development process, and quality requirements followed in the design;
- Strategies for all phases of testing, including commissioning;
- Design and development of verification and validation methods and results;
- Operating procedures for all normal operation states and modes;
- Emergency operating procedures, and severe accident guidelines, to cover postulated accident scenarios and design extension conditions;

- Recommendations and purchasing specifications for provision of spare parts and components;
- Security design features and their application.¹⁰

2.91. Documentation of processes and requirements for acquisition and supply, design, fabrication activities, software code, and verification and validation should be available for assessment by the operating organization, regulatory body or independent third parties acting for these organizations (see paras 9.100–9.103).

LIFE CYCLE ACTIVITIES

Requirements specification

2.92. The requirements for the overall I&C, each individual I&C system and I&C components should be documented in an appropriate form.

2.93. The combination of requirements of the full set of individual I&C systems should fulfil the design basis established for the overall I&C.

2.94. The requirements for the overall I&C and each individual I&C system should be derived from the I&C design basis.

2.95. Section 3 discusses the derivation and content of the overall I&C design basis.

2.96. The system and component requirements should specify, as applicable, the following:

- What each individual I&C system or component is to do;
- The relations between inputs and outputs for each function in each plant state and each plant operating mode;
- The minimum precision and accuracy and the maximum time response for measurements, control functions and displays;

¹⁰ If the design makes use of assumptions about the operating organization's operational security policies and practices (including policies and practices relating to computer security), these are to be communicated to the user. It might be appropriate to include elements of such descriptions in separate documents, so that their distribution can be more restricted than other system information.

- The system interfaces (e.g. between the system and the operator, and with other systems);
- Self-supervision features, including their required timing performance (including fault detection times and recovery times);
- The actions to be taken by the I&C system upon detection of faults by means of self-supervision;
- Security features (such as validity checks, specific computer security controls and features that allow systems to inherit the security controls in their environments and to inherit access privileges);
- The level of reliability and availability to be achieved and any supporting requirements necessary to ensure that this is achieved;¹¹
- Facilities and features required for maintenance;
- Design constraints;¹²
- Safe response to particular failure modes;
- Robustness to the full range of operating environments associated with normal conditions and accident conditions on the plant and foreseeable internal and external hazards.

2.97. Where design constraints are necessary, they should be specified, justified and traceable.

2.98. Security design requirements for digital systems should take account of the results of a security risk assessment and should be consistent with the characteristics of the operating organization's security policies.

2.99. Specific processes should be used to manage requirements throughout the life cycle and to ensure that all requirements are fulfilled, verified, validated and implemented.

2.100. Requirements engineering is a specific process for ensuring that the safety goals of I&C systems are addressed by the design.

¹¹ The level of reliability and availability might be defined quantitatively or qualitatively, for example, in terms of the supporting requirements referred to above, such as requirements for implementation of specific reliability strategies, requirements for characteristics of the development process or requirements for compliance with specified standards.

¹² Examples of design constraints include constraints to support independence or diversity requirements.

2.101. Requirements should be established and documented using a predetermined combination of techniques commensurate with the system's importance to safety.

2.102. Techniques for establishing and documenting requirements might include the use of specification languages that have well defined syntax and semantics, models, analysis and review.

2.103. As far as possible, requirements should be written in terms of what needs to be achieved rather than how the requirements are to be designed and implemented.

2.104. Requirements should be described in terms understandable to all of the parties concerned (e.g. the licensee, suppliers and designers).

2.105. Documentation of requirements should refer to, include or be complemented by additional information, for example, background information for specific requirements, risk considerations, recommendations for the design of functions or safety features, to the extent necessary to ensure that the requirements are fully understood by their target audience.

2.106. Requirements that have a potential impact on safety should be identified as such.

2.107. The origin of, and rationale for, every requirement should be defined to facilitate verification, validation, traceability to higher-level documents and demonstration that all relevant design basis requirements have been taken into account.

Selection of predeveloped items

2.108. Predeveloped items should be appropriately qualified in accordance with the guidance given in paras 6.78–6.134.

2.109. Predeveloped items include hardware devices, predeveloped software, commercial off the shelf devices, digital devices composed of both hardware and software, hardware devices configured with hardware definition language or predeveloped functional blocks usable in hardware description language.

2.110. Reference [11] provides more detail about the use of commercial off the shelf devices.

2.111. Any functions of a predeveloped item that are not used in implementing an I&C safety system should be shown not to interfere unacceptably with the system's safety functions.

2.112. Where feasible, predeveloped items should be configured such that unused functions are disabled.

2.113. Often, predeveloped items selected are commercial off the shelf devices. Use of commercial off the shelf devices might reduce costs and design effort. Furthermore, there may be no device specific for nuclear power plants available and use of a well proven commercial product could be more effective or safer than development of a new item.

2.114. Commercial off the shelf devices tend to be more complex, may have unintended functionalities and often become obsolete in a shorter time. They will often have functions that are not needed in the nuclear power plant application. Qualification of a commercial off the shelf device could be more difficult because commercial development processes may be less transparent and controlled than those described in this Safety Guide. Often, qualification is impossible without cooperation from the vendor. The difficulty associated with acceptance of a commercial off the shelf device may often lie with the unavailability of the information to demonstrate quality and reliability.

2.115. In the process of deciding whether to use commercial off the shelf devices or not, the licensee should consider the maintenance of their qualification during the lifetime of the plant.

2.116. For example, there might be frequent design changes of the product line, such as changes to subcomponents, new firmware versions, new manufacturing processes or new software versions. This may pose challenges to the vendor as well as the plant configuration management in properly identifying such modifications, especially with regard to I&C maintenance and management of spare parts. In some cases, operating organizations have purchased a 'lifetime supply' of spares of a specific version to avoid the possibility that a specific component or version becomes unavailable for purchase.

2.117. Predeveloped items should have documentation that gives the information necessary for their use in the I&C system.

Design and implementation of instrumentation and control systems

2.118. The design of the overall I&C architecture and the individual I&C systems should result from a systematic, stepwise decomposition of the required functionality plus other requirements.

2.119. The system requirements that are to be satisfied by an I&C system should be allocated to an appropriate combination of hardware, devices configured with hardware description language, and software (if present).

2.120. Hardware might include integrated circuits specific to certain applications. Software might include pre-existing software and firmware, such as the operating system, software to be developed or software to be produced by configuring predeveloped software. The refined requirements might also have to take into account lower level design decisions made in respect of parts outside of the I&C system, for example, the type and performance of actuated devices.

2.121. The implementation of requirements that are not important to safety should be shown not to interfere with functions important to safety.

2.122. Design rules should be established to ensure that the internal logic of each I&C system is amenable to verification and validation.

2.123. The design should take into account I&C parameters that need to be configurable or verified and validated during operation, and should provide the means to do so (e.g. trip settings for the reactor protection system, calibration constants and software configuration settings).

System integration

2.124. System integration:

- Should address all interfaces between the components being integrated, such as between the hardware and software or between software modules;
- Should confirm that requirements for the interfaces between the various components of the system are met;
- Should confirm that the components, subassemblies and subsystems operate as designed in the integrated system to enable the system to meet its specified requirements, including requirements covering out-of-range values, exception handling and timing.

2.125. A consistent configuration of verified modules (hardware and software) should be available prior to the beginning of system integration.

2.126. Software tools 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 on-site in operation to facilitate configuration control and traceability between installed components and validated components.

2.127. A documented traceability analysis should be used to demonstrate that the system integration is complete with respect to the system design specification and that the objectives of para. 2.124 have been met.

System validation

2.128. System validation should be performed for each individual I&C system and for the integrated set of I&C systems.

2.129. For the purpose of this Safety Guide, system validation ends when installation of the system into the plant is complete. If some additional elements of system validation need to be performed after the system is installed in the plant, these may be included in commissioning tests, provided that the results are included in validation test records and that independence, as defined in paras 2.71 and 2.72, is maintained between the design team and the validation team.

2.130. The system that is subjected to testing for the purposes of validation should be representative of the final configuration of the I&C system at the site.

2.131. The software that is subjected to system validation should be identical to the software that will be used in operation.

2.132. System validation should demonstrate that the system meets all of the requirements under all possible interface conditions and all possible load conditions.

2.133. Modes of operation and interactions between I&C systems and the plant that could not be readily tested during system validation should be tested during commissioning, or should be validated through supplementary analysis.

2.134. System validation should cover:

- All parts of the system;
- The full ranges of interface signals¹³, including out-of-range values;
- Exceptions handling;
- Set point accuracy and hysteresis;
- All modes of plant and system operation, including transitions between modes;
- Recovery after power failure;
- Timing;
- Robustness and fault tolerance.

2.135. The system validation tests should involve variation of all inputs, i.e. dynamic testing should be used.

2.136. The dynamic tests should use realistic scenarios that are representative of plant parameter variations that would place demands on the I&C system and that are based on an analysis of the possible plant scenarios.

2.137. The functional tests should be designed to cover all behaviours allowed by the functional requirements. The structural coverage of functional tests should be justified taking account of the functional requirements.

2.138. Validation testing using statistical techniques should be considered.

2.139. The use of simulators for system validation should be considered.

2.140. The system operation manuals and appropriate parts of the maintenance manuals should be validated during system validation to the maximum extent possible.

2.141. A documented traceability analysis should demonstrate that the system validation is complete with respect to the specification of system requirements and that the objectives of paras 2.132 and 2.134 have been met.

¹³ Interface signals include, for example, inputs and outputs to or from other systems, sensors, actuators and operator interfaces.