

IAEA Safety Standards

for protecting people and the environment

Instrumentation and Control Systems and Software Important to Safety for Research Reactors

Specific Safety Guide

No. SSG-37



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.

INSTRUMENTATION AND
CONTROL SYSTEMS AND
SOFTWARE IMPORTANT TO
SAFETY FOR
RESEARCH REACTORS



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

AFGHANISTAN	GERMANY	OMAN
ALBANIA	GHANA	PAKISTAN
ALGERIA	GREECE	PALAU
ANGOLA	GUATEMALA	PANAMA
ARGENTINA	GUYANA	PAPUA NEW GUINEA
ARMENIA	HAITI	PARAGUAY
AUSTRALIA	HOLY SEE	PERU
AUSTRIA	HONDURAS	PHILIPPINES
AZERBAIJAN	HUNGARY	POLAND
BAHAMAS	ICELAND	PORTUGAL
BAHRAIN	INDIA	QATAR
BANGLADESH	INDONESIA	REPUBLIC OF MOLDOVA
BELARUS	IRAN, ISLAMIC REPUBLIC OF	ROMANIA
BELGIUM	IRAQ	RUSSIAN FEDERATION
BELIZE	IRELAND	RWANDA
BENIN	ISRAEL	SAN MARINO
BOLIVIA, PLURINATIONAL STATE OF	ITALY	SAUDI ARABIA
BOSNIA AND HERZEGOVINA	JAMAICA	SENEGAL
BOTSWANA	JAPAN	SERBIA
BRAZIL	JORDAN	SEYCHELLES
BRUNEI DARUSSALAM	KAZAKHSTAN	SIERRA LEONE
BULGARIA	KENYA	SINGAPORE
BURKINA FASO	KOREA, REPUBLIC OF	SLOVAKIA
BURUNDI	KUWAIT	SLOVENIA
CAMBODIA	KYRGYZSTAN	SOUTH AFRICA
CAMEROON	LAO PEOPLE'S DEMOCRATIC REPUBLIC	SPAIN
CANADA	LATVIA	SRI LANKA
CENTRAL AFRICAN REPUBLIC	LEBANON	SUDAN
CHAD	LESOTHO	SWAZILAND
CHILE	LIBERIA	SWEDEN
CHINA	LIBYA	SWITZERLAND
COLOMBIA	LIECHTENSTEIN	SYRIAN ARAB REPUBLIC
CONGO	LITHUANIA	TAJIKISTAN
COSTA RICA	LUXEMBOURG	THAILAND
CÔTE D'IVOIRE	MADAGASCAR	THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
CROATIA	MALAWI	TOGO
CUBA	MALAYSIA	TRINIDAD AND TOBAGO
CYPRUS	MALI	TUNISIA
CZECH REPUBLIC	MALTA	TURKEY
DEMOCRATIC REPUBLIC OF THE CONGO	MARSHALL ISLANDS	UGANDA
DENMARK	MAURITANIA	UKRAINE
DJIBOUTI	MAURITIUS	UNITED ARAB EMIRATES
DOMINICA	MEXICO	UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
DOMINICAN REPUBLIC	MONACO	UNITED REPUBLIC OF TANZANIA
ECUADOR	MONGOLIA	UNITED STATES OF AMERICA
EGYPT	MONTENEGRO	URUGUAY
EL SALVADOR	MOROCCO	UZBEKISTAN
ERITREA	MOZAMBIQUE	VENEZUELA, BOLIVARIAN REPUBLIC OF
ESTONIA	MYANMAR	VIET NAM
ETHIOPIA	NAMIBIA	YEMEN
FIJI	NEPAL	ZAMBIA
FINLAND	NETHERLANDS	ZIMBABWE
FRANCE	NEW ZEALAND	
GABON	NICARAGUA	
GEORGIA	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-37

INSTRUMENTATION AND CONTROL SYSTEMS AND SOFTWARE IMPORTANT TO SAFETY FOR RESEARCH REACTORS

SPECIFIC SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2015

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, 2015

Printed by the IAEA in Austria

June 2015

STI/PUB/1692

IAEA Library Cataloguing in Publication Data

Instrumentation and control systems and software important to safety for research reactors. — Vienna : International Atomic Energy Agency, 2015.

p. ; 24 cm. — (IAEA safety standards series, ISSN 1020-525X ; no. SSG-37)

STI/PUB/1692

ISBN 978-92-0-102615-6

Includes bibliographical references.

1. Nuclear reactors — Safety measures.
2. Nuclear engineering— Instruments.
3. Nuclear reactors — Control. I. International Atomic Energy Agency. II. Series.

IAEAL

15-00975

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.

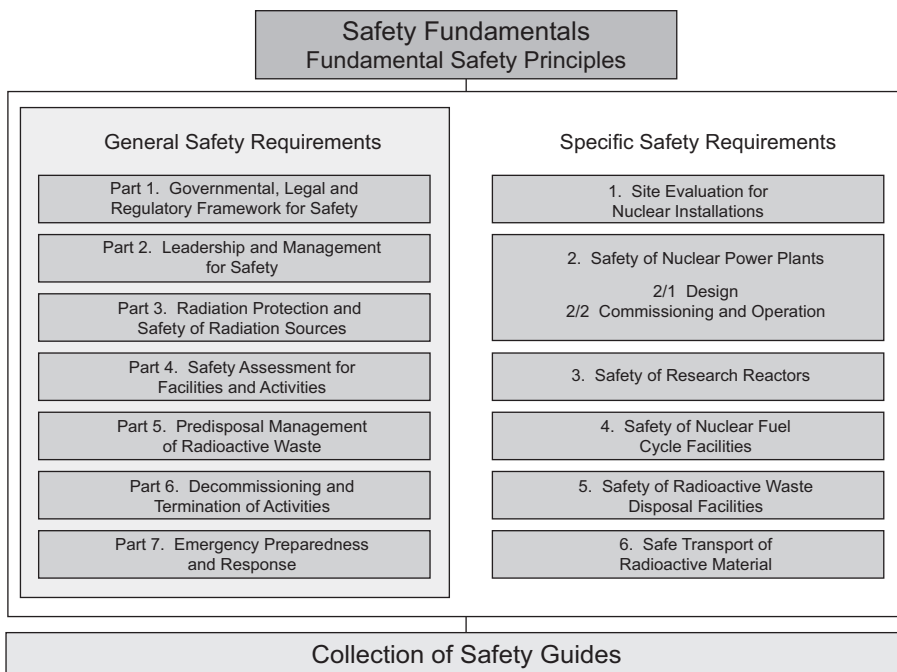


FIG. 1. The long term structure of the IAEA Safety Standards Series.

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

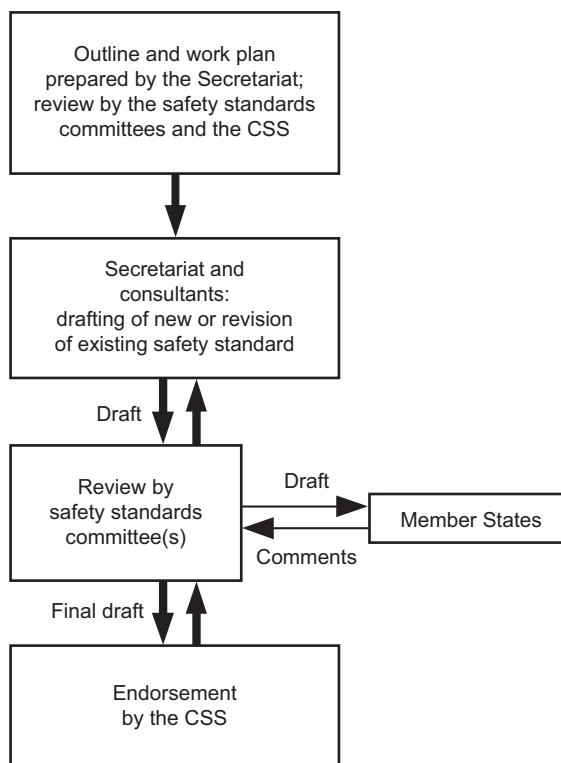


FIG. 2. The process for developing a new safety standard or revising an existing standard.

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 (1.1–1.2)	1
	Objective (1.3)	1
	Scope (1.4–1.6)	1
	Structure (1.7)	2
2.	SAFETY CLASSIFICATION OF INSTRUMENTATION AND CONTROL SYSTEMS	2
	General considerations (2.1–2.4)	2
	Methods of classification (2.5–2.6)	4
	Design, construction, commissioning, operation and maintenance of instrumentation and control systems (2.7–2.9) ...	5
3.	OVERALL INSTRUMENTATION AND CONTROL SYSTEM ARCHITECTURE	5
	General (3.1–3.3)	5
	Defence in depth (3.4–3.6)	6
	Independence (3.7–3.10)	7
	Consideration of common cause failure (3.11–3.14)	7
	Architectural design of the instrumentation and control system (3.15–3.21)	8
4.	DESIGN GUIDELINES AND CRITERIA	11
	General (4.1–4.2)	11
	Design basis (4.3–4.4)	12
	Design for reliability (4.5–4.34)	13
	Design considerations for ageing (4.35–4.38)	17
	Consideration of the safety and security interface in the design (4.39–4.51)	18
	Equipment qualification (4.52–4.70)	20
	Testing and testability (4.71–4.97)	23
	Maintainability (4.98–4.101)	28
	Design analysis (4.102–4.104)	28

Safety system settings (4.105–4.106)	30
Identification of items important to safety (4.107)	30
5. SYSTEM SPECIFIC DESIGN GUIDELINES	31
Sensing devices (5.1–5.7)	31
Reactor protection system (5.8–5.23)	32
Other instrumentation and control systems important to safety (5.24–5.49)	35
Power supplies of instrumentation and control systems (5.50–5.52)	39
6. OPERATION	40
Operational limits and conditions (6.1–6.5)	40
Control of access to systems important to safety (6.6–6.13)	41
Maintenance, testing, surveillance and inspection of instrumentation and control systems and components important to safety (6.14–6.15)	42
Provisions for removal from service for testing or maintenance (6.16–6.18)	43
Extended shutdown (6.19)	43
7. HUMAN FACTORS ENGINEERING AND THE HUMAN–MACHINE INTERFACE	43
General considerations (7.1–7.4)	43
Criteria for human factors engineering and design for the human–machine interface (7.5–7.28)	44
8. COMPUTER BASED SYSTEMS AND SOFTWARE	48
General considerations (8.1–8.5)	48
Computer based systems and software design considerations (8.6–8.26)	48
Project planning (8.27–8.39)	51
Specification of requirements for computer based systems (8.40–8.57)	53
Verification and analysis (8.58–8.64)	56
Computer system integration (8.65–8.77)	56
Operation, maintenance and modification (8.78–8.82)	58

9. CONFIGURATION MANAGEMENT (9.1–9.3) 59

10. MODIFICATION AND MODERNIZATION OF
INSTRUMENTATION AND CONTROL SYSTEMS (10.1–10.30)... 60

REFERENCES 65

ANNEX: INSTRUMENTATION AND CONTROL SYSTEMS
THAT CAN BE USED IN A RESEARCH REACTOR..... 67

CONTRIBUTORS TO DRAFTING AND REVIEW 75

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide supplements and elaborates upon the safety requirements for design and operation of instrumentation and control systems for research reactors that are established in sections 6 and 7 of IAEA Safety Standards Series No. NS-R-4, Safety of Research Reactors [1].

1.2. Over the lifetime of a research reactor, one or more refurbishments of instrumentation and control systems would be expected. Reasons for modernization projects for instrumentation and control systems of a research reactor might be obsolescence or ageing, improvement of maintainability and reliability, reactor reconstruction and upgrading, new utilization or experiments and enhancement of safety.

OBJECTIVE

1.3. The objective of this Safety Guide is to provide recommendations and guidance on instrumentation and control systems important to safety for research reactors, including instrumentation and control system architecture and associated components, from sensors to actuators, operator interfaces and auxiliary equipment. This Safety Guide is intended for use by regulatory bodies and by all organizations involved in the design and operation of research reactors, including the operating organizations, suppliers of instrumentation and control systems, and other organizations involved in a research reactor project.

SCOPE

1.4. This Safety Guide provides recommendations and guidance on the safety classification, design, implementation, qualification and operation of instrumentation and control systems important to safety for research reactors to achieve compliance with NS-R-4 [1]. This Safety Guide also addresses safety and security interface issues.

1.5. The recommendations and guidance apply to both the design and configuration management of instrumentation and control systems for new research reactors and the modernization of the instrumentation and control systems of existing research reactor facilities.

1.6. This Safety Guide also provides recommendations and guidance on human factors engineering and human–machine interfaces, and for computer based systems and software for use in instrumentation and control systems important to safety.

STRUCTURE

1.7. Section 2 discusses the identification of instrumentation and control functions and systems, the method and the basis for safety classification into safety functions and systems and safety related functions and systems. Section 3 gives guidance on how instrumentation and control systems are to be arranged into a hierarchy. Sections 4 and 5 provide an overview on meeting the general and specific design requirements for instrumentation and control systems. The operational aspects of instrumentation and control systems are presented in Section 6. Section 7 expands on the guidance given in Section 4 in the area of human–machine interfaces. Section 8 provides guidance on design aspects and other aspects of computer based systems and software. Section 9 provides guidance on configuration management for instrumentation and control systems. Section 10 presents considerations in the modification and modernization of instrumentation and control systems. The Annex identifies instrumentation and control systems that can be used in a research reactor.

2. SAFETY CLASSIFICATION OF INSTRUMENTATION AND CONTROL SYSTEMS

GENERAL CONSIDERATIONS

2.1. Instrumentation and control functions, systems and components may be classified into two categories: items important to safety and items not important to safety (see Fig. 1 and the Annex). Functions, systems and components important to safety are those which contribute to:

Plant equipment				
Items important to safety				Items not important to safety
Safety systems			Safety related items	
Protection systems	Safety actuation systems	Safety system support features		
Initiation I&C for: Reactor trip Emergency core cooling Decay heat removal Dynamic confinement isolation Confinement heat removal I&C for command & monitoring: Safety parameter command and display consoles and panels	Actuation I&C for: Reactor trip Emergency core cooling Decay heat removal Confinement isolation Confinement heat removal	I&C for: Emergency power supply		
			I&C for: Off-line water demineralizing plant Off-line water treatment systems Some plant auxiliary systems Comfort HVAC for non-controlled/non-supervised areas	

Note: CCTV — closed circuit television; HVAC — heating, ventilation and air-conditioning; I&C — instrumentation and control.

FIG. 1. Examples of instrumentation and control systems of a research reactor classified according to their importance to safety.

- Safely shutting down the reactor and maintaining it in a safe shutdown condition in and after operational states and accident conditions;
- Removing residual heat from the reactor core after shutdown, in all operational states and accident conditions;
- Preventing, or reducing the potential for, releases of radioactive material and ensuring that any releases are within authorized limits in all operational states and within acceptable limits in and after accidents;
- Permitting the safe operation of the reactor.

2.2. Instrumentation and control systems not important to safety are those used to accomplish functions supporting the operation of the facility, while having no impact on the safety of the reactor.

2.3. Systems and components important to safety are further categorized into either safety systems or safety related systems:

- (a) Safety systems consist of the protection system, the safety actuation systems and the safety system support features.
- (b) Safety related systems are systems important to safety that are not part of a safety system, such as systems for monitoring the availability of safety systems.

2.4. For instrumentation and control systems important to safety, a graded approach to the application of the requirements of NS-R-4 [1] may be used, but the extent of grading should be clearly justified in the safety analysis report (the factors to be considered can be found in para. 1.14 of NS-R-4 [1]). Additional recommendations and guidance on the application of the graded approach are provided in IAEA Safety Standards Series No. SSG-22, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors [2].

METHODS OF CLASSIFICATION

2.5. The method for classifying the safety significance of a structure, system or component should be based primarily on deterministic methods, complemented by engineering judgement and where appropriate by probabilistic methods, if available. For instrumentation and control systems, the basis for such a classification should consider:

- (a) The safety function(s) to be performed by the instrumentation and control system.
- (b) The consequences of failure of the instrumentation and control system (failure or faulty performance of the function(s)). This includes the potential for the instrumentation and control system itself (i.e. the fail-safe modes of instrumentation and control systems) to cause an initiating event and the combination of the probability and consequences of such an initiating event (i.e. frequency of failure and the possible radiological consequences).
- (c) The estimated frequency or probability (if available) that the instrumentation and control system will be called upon to perform a safety function.

- (d) Following a postulated initiating event, the time at which or the period for which the instrumentation and control system will be called upon to operate.

2.6. The instrumentation and control functions necessary to mitigate the consequences of design extension conditions could be assigned to a lower safety class than the functions necessary to control anticipated operational occurrences and design basis accident conditions to reach a controlled state of the research reactor.

DESIGN, CONSTRUCTION, COMMISSIONING, OPERATION AND MAINTENANCE OF INSTRUMENTATION AND CONTROL SYSTEMS

2.7. All instrumentation and control systems and equipment should be designed, constructed, commissioned, operated and maintained in such a manner that their specification, their verification and validation process, and their quality and reliability are commensurate with their safety classification. The specifications should consider sufficient margins for their safety system design. These margins should be verified at both component level and system level by testing and analysis.

2.8. All instrumentation and control systems and equipment performing functions important to safety should have appropriately designed interfaces with systems and equipment of different safety classes in order to ensure (e.g. by using isolation devices) that any failure in a system classified in a lower safety class (with less stringent requirements) will not propagate to a system classified in a higher safety class. Equipment that fulfils the function to prevent such a propagation of failure should be treated as being in the higher class.

2.9. The safety class of an instrumentation and control system should be the same as the safety class of the system or equipment that it controls or monitors.

3. OVERALL INSTRUMENTATION AND CONTROL SYSTEM ARCHITECTURE

GENERAL

3.1. The research reactor should be provided with sufficient instrumentation and control systems for ensuring the safety of the facility in normal operation, including startup, operation at power, shutting down, refuelling and maintenance,

and in accident conditions. In particular, the instrumentation and control systems should be able to automatically initiate reactor shutdown, emergency core cooling, residual heat removal and the confinement of radioactive material, although manual operation action may be permitted as described in para. 5.14. The instrumentation and control system architecture should provide sufficient capabilities to cover all anticipated operational occurrences and post-event conditions.

3.2. The instrumentation and control system architecture has to fulfil the safety objectives and design requirements established in paras 2.2–2.7, 6.1–6.43, 6.61–6.65, 6.94–6.105 and 6.136–6.144 of NS-R-4 [1]. The instrumentation and control system architecture should support all the instrumentation and control functions necessary to ensure the safety of the facility.

3.3. The instrumentation and control system architecture provides high level definition of the instrumentation and control systems, the assignment of instrumentation and control functions to these systems, and the communications (interfaces) between instrumentation and control systems and the facility operators and users. Modern instrumentation and control systems are more highly integrated than in the past. The architecture of highly integrated systems should be carefully considered to ensure proper implementation of the defence in depth concept. A good architectural design is characterized by a rational allocation of functions, only in the systems where they are needed. The identification of the different and individual instrumentation and control systems that can be included in a particular research reactor facility depends on the type of reactor, its purpose and its operation modes. These different instrumentation and control systems are described in the Annex.

DEFENCE IN DEPTH

3.4. As stated in para. 2.5 of NS-R-4 [1]:

“Application of the concept of defence in depth throughout design and operation provides a graded protection against a wide variety of transients, anticipated operational occurrences and accidents, including those resulting from equipment failure or human action within the installation, and events that originate outside the installation.”

3.5. The design of the instrumentation and control system should incorporate the defence in depth concept. The levels of defence should be independent as far as is practicable (see also Ref. [3]).

3.6. The instrumentation and control system architecture should:

- (a) Implement a defence in depth concept. For instrumentation and control, defence in depth includes implementing successive instrumentation and control functions designed to limit the consequences of a postulated initiating event despite the failure of the instrumentation and control functions designed to respond first.
- (b) Not compromise the strategy to meet the defence in depth concept of the facility design.

INDEPENDENCE

3.7. Independence is intended to prevent the propagation of failures from the item affected by the failure to other redundancies, or from one system to another system independent of the safety class to which they belong.

3.8. The instrumentation and control system architecture should not compromise the independence in effect at the different levels of defence in depth.

3.9. Safety systems should be independent of systems of lower safety classification to ensure that the safety systems can perform their safety functions during and following any postulated initiating event that requires these functions without any interference or degradation from systems of lower safety classification.

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

CONSIDERATION OF COMMON CAUSE FAILURE

3.11. A common cause failure is defined as the failure of two or more structures, systems and components due to a single event or cause [4]. Common cause failure might happen, for example, because of:

- Human errors in operation or maintenance;
- A design deficiency;
- A manufacturing deficiency;
- Inadequate specification;

- Inadequate qualification for or protection against internal or external hazards, a human induced event, high voltages, data errors, data communication errors, or failure propagation between systems or components.

3.12. Latent failures and common failure modes that could potentially result in a common failure of the redundancies should be identified. Justification should be provided for those sources of common cause failure between systems or individual components that the operating organization does not consider credible. Justification that a common cause failure may not need to be considered can be based, for example, on the assigned level of defence in depth of the instrumentation and control function, the dependability of the components or the technology applied.

3.13. An analysis should be conducted of the consequences of each postulated initiating event within the scope of the safety analysis in combination with common cause failures that will prevent a protection system from performing the necessary safety functions.

3.14. The design of systems and components should take due account of the potential for common cause failures of items important to safety to determine how the concepts of diversity, physical separation, and electrical and functional isolation have to be applied to achieve the necessary reliability.

ARCHITECTURAL DESIGN OF THE INSTRUMENTATION AND CONTROL SYSTEM

3.15. The instrumentation and control system architecture:

- (a) Should provide all instrumentation and control functions necessary to ensure the safe operation of the facility and to manage anticipated operational occurrences and accident conditions.
- (b) Should provide the systems necessary to support the defence in depth strategy of the facility.
- (c) Should provide preferably a hierarchical system design where instrumentation and control systems that belong to safety systems keep the highest priority to perform the safety functions for which they have been designed. In this way, other systems of lower safety class are not able to prevent the actions initiated by safety systems (i.e. shutdown of the reactor).

- (d) Should provide a suitable arrangement of systems and components so that they can be adequately tested and maintained at regular intervals in accordance with their importance to safety.
- (e) Should divide the overall instrumentation and control system into individual systems as necessary:
 - (i) To fulfil design basis requirements for independence between functions at different levels of the defence in depth concept;
 - (ii) To adequately separate systems and functions of different safety classes;
 - (iii) To establish the redundancy necessary to fulfil design basis reliability requirements;
 - (iv) To support the compliance of safety systems with the single failure criterion and the fail-safe criterion;
 - (v) To provide the necessary information and operator controls in the main control room and the supplementary control room (if applicable);
 - (vi) To provide the automatic controls necessary to maintain and limit the process variables important to safety within the specified normal operational ranges.
- (f) Should define the interfaces between the individual instrumentation and control systems.
- (g) Should consider special precautions in relation to the utilization and modification of the research reactor to ensure that the configuration of the reactor, as well as the configuration of the instrumentation and control system, is known at all times throughout the lifetime of the reactor.

3.16. The inputs to the design process for the instrumentation and control system architecture should refer to the documents on the safety design basis for the facility, which should provide the following information:

- (a) The defence in depth concept of the facility;
- (b) The groups of functions to be provided to address postulated sequences of initiating events;
- (c) The safety classification and the functional and performance requirements of the facility functions important to safety;
- (d) The role of automation and prescribed operator actions in the management of anticipated operational occurrences and accident conditions;
- (e) The assignment of functions to operators and to automatic means;
- (f) The information to be provided to the operators;
- (g) The priority criteria between automatically initiated and manually initiated actions;

- (h) National requirements, including those for licensing of instrumentation and control systems;
- (i) Requirements on the operating organization with respect to operational features (i.e. the design of the instrumentation and control system as it affects the interface with facility operators) for systems important to safety.

3.17. The instrumentation and control systems should be designed in a ‘top-down’ architecture (see Fig. 2) having different levels of monitoring, processing, acquisition and actuation, sensors and actuator drivers. The monitoring functions should be allocated at the supervision level; the calculation, algorithms, and safety and process functions should be allocated at the control level; the acquisition and actuation functions should be allocated at the field level; and sensors and actuator drivers should be located at the facility level.

3.18. The use of diversity, redundancy and independence (i.e. physical separation, and electrical and functional isolation) in the architecture of the instrumentation and control systems should be consistent with the safety classification of each instrumentation and control system, and with the defence in depth concept, both for the overall facility and for the instrumentation and control system. In the case of redundancy, other factors such as reliability (i.e. the probability that a system or component will meet its minimum performance requirements when called upon to do so [4]) or the availability of instrumentation and control systems should be considered.

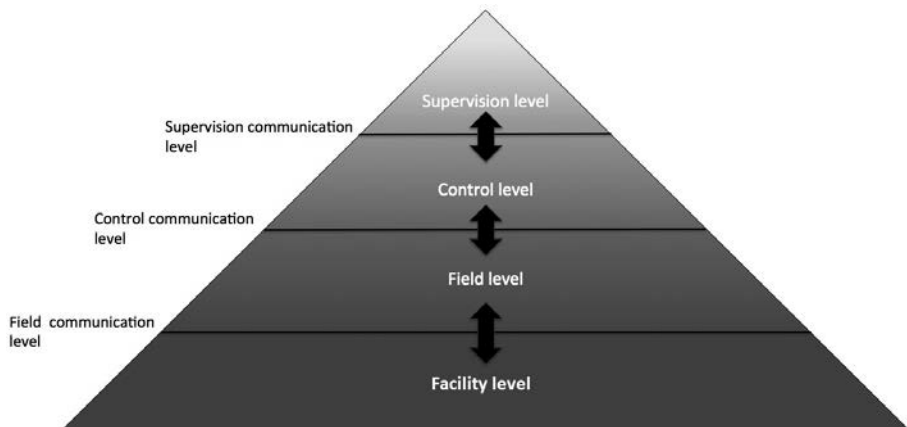


FIG. 2. ‘Top-down’ architecture of the instrumentation and control systems.

3.19. The ‘top-down’ hierarchy architecture for the instrumentation and control systems requires the inclusion of three independent levels of communication to provide interfaces for communication between the different architectural levels and the reactor systems and facility systems, namely:

- (a) Supervision level of communication;
- (b) Control level of communication;
- (c) Field level of communication.

3.20. The features mentioned in para. 3.19 should be used in the design of the different architectural levels to reduce the likelihood of dependent failures at these levels.

3.21. The instrumentation and control system should have a fail-safe design such that no malfunction within the system caused solely by variations of external conditions within the ranges detailed in the design basis would result in an unsafe condition or failure.

4. DESIGN GUIDELINES AND CRITERIA

GENERAL

4.1. Instrumentation and control systems should fully implement the requirements of their design bases. The origin of, and the objective for, every requirement should be specified and documented to facilitate verification and traceability to higher level documents and as a demonstration that all relevant design requirements have been accounted for.

4.2. The design of the instrumentation and control systems should be as simple as possible to fulfil their functions. Simplicity of design leads to fewer components, simpler interfaces, easier verification and validation, and easier maintenance of the hardware and software. Adequate analysis of the design requirements is an effective means to achieve simplicity of design.

DESIGN BASIS

4.3. Each instrumentation and control system important to safety for the research reactor should have a design basis that specifies the following:

- (a) The facility states (operational states and accident conditions) in which the system is required;
- (b) The various configurations of the facility and experimental configurations that the instrumentation and control system is required to accommodate;
- (c) Functionality requirements for each facility state, including extended shutdown;
- (d) Performance requirements, including the guaranteed response time for safety functions;
- (e) The facility conditions during which manual control is allowed for each manual protective action;
- (f) Postulated initiating events to which the system is required to respond;
- (g) The variables, or combination of variables, to be monitored, the control actions required, and the identification of actions to be performed automatically, manually or both;
- (h) The ranges, rates of change, and required accuracy of input and output signals of the system;
- (i) Constraints on the values of process variables in all postulated conditions;
- (j) Requirements for periodic testing, self-diagnostics and maintenance;
- (k) System reliability levels, which may be specified using deterministic criteria, probabilistic criteria or both;
- (l) Requirements for system availability;
- (m) The range of transient and steady state environmental conditions under which the system is required to perform functions important to safety;
- (n) The range of environmental conditions, including those hazards potentially arising from natural phenomena, under which the system is required to perform functions important to safety;
- (o) Conditions with the potential to functionally degrade the performance of systems important to safety and the provisions to be made to retain their capability of performance;
- (p) The whole lifetime of the facility including accident conditions and conditions following an accident;
- (q) Operational constraints.