IAEA Safety Standards

for protecting people and the environment

Human Factors Engineering in the Design of Nuclear Power Plants

Specific Safety Guide

No. SSG-51

IAEA
International Atomic Energy Agency

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

https://www.iaea.org/resources/safety-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.

HUMAN FACTORS ENGINEERING IN THE DESIGN OF NUCLEAR POWER PLANTS

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

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

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

IAEA SAFETY STANDARDS SERIES No. SSG-51

HUMAN FACTORS ENGINEERING IN THE DESIGN OF NUCLEAR POWER PLANTS

SPECIFIC SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

COPYRIGHT NOTICE

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

Printed by the IAEA in Austria
June 2019
STI/PUB/1843

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Human factors engineering in the design of nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2019. | Series: IAEA safety standards series, ISSN 1020–525X ; no. SSG-51 | Includes bibliographical references.
Identifiers: IAEAL 19-01229 | ISBN 978–92–0–100419–2 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Human factors. | Nuclear power plants — Safety measures. | Human engineering.
Classification: UDC 621.039.58 | STI/PUB/1843

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 measures[1] 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.

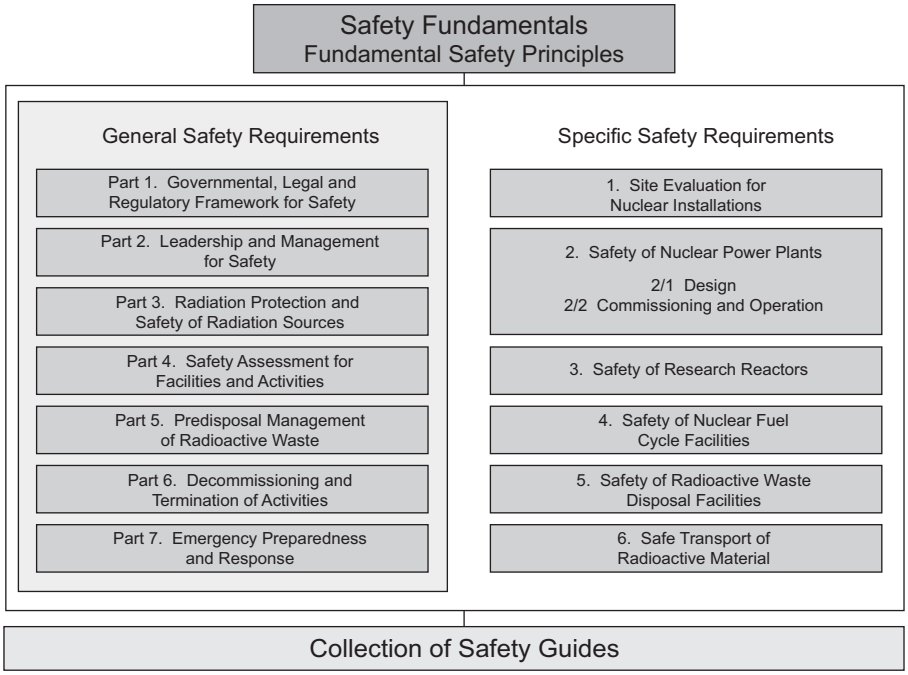

FIG. 1. The long term structure of the IAEA Safety Standards Series.

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 five safety standards committees, for emergency preparedness and response (EPReSC) (as of 2016), 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

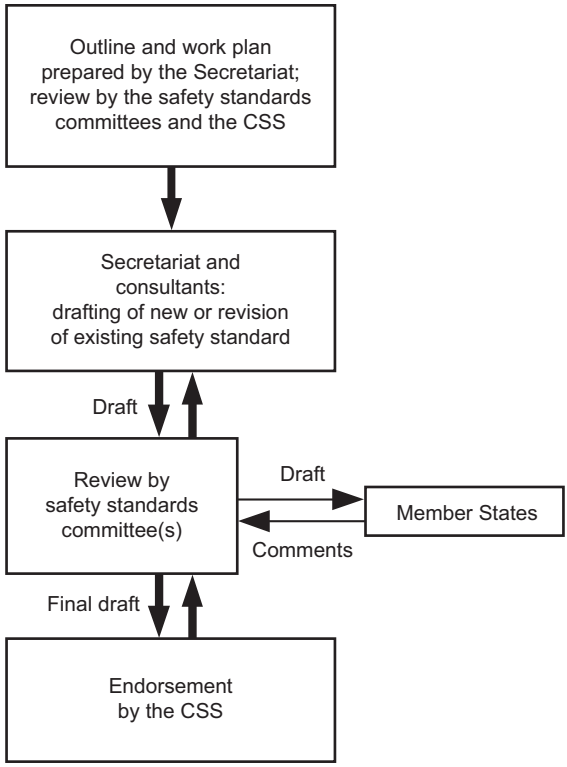

FIG. 2. The process for developing a new safety standard or revising an existing standard.

the Commission on Safety Standards is appointed by the Director General and 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

BACKGROUND

1.1. This Safety Guide provides recommendations on the application of human factors engineering (HFE)[1] to meet the requirements established in IAEA Safety Standards Series Nos SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [1], SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [2], and GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities [3].

1.2. This Safety Guide takes into account developments, experience and practices in integrating HFE into the design of nuclear power plants throughout their lifetime. It references and takes into account other IAEA Safety Standards Series publications that are relevant and related to the integration of HFE into design. These include IAEA Safety Standards Series No. GSR Part 2, Leadership and Management for Safety [4], and its supporting Safety Guides: IAEA Safety Standards Series Nos GS-G-3.1, Application of the Management System for Facilities and Activities [5], and GS-G-3.5, The Management System for Nuclear Installations [6].

1.3. The main topical areas for which this Safety Guide provides guidance are:

- The HFE processes to be applied in the design of human–machine interface (HMI) for all plant states, for achieving compliance with the requirements established in SSR-2/1 (Rev. 1) [1];
- Integration of HFE into the design of a nuclear power plant throughout its lifetime for achieving compliance with the requirements established in GSR Part 2 [4];
- Human performance monitoring and evaluation throughout the lifetime of the nuclear power plant;
- Integration of HFE into safety processes, applications and product selection.

[1] 'Human factors engineering' is engineering in which factors that could influence human performance and that could affect safety are understood and are taken into account, especially in the design and operation of facilities.

1.4. This Safety Guide considers HFE aspects for several important processes linked to design, such as:

— Development and review of the safety analysis report;
— Plant modifications for achieving compliance with the requirements established in SSR-2/2 (Rev. 1) [2];
— Periodic safety review.

1.5. This Safety Guide considers relevant HFE aspects for the design and use of computerized procedures.

1.6. This Safety Guide considers relevant HFE aspects for the selection, procurement, integration and use of several products in existing plant systems, such as:

— Personal protective equipment (e.g. personal protective equipment used during maintenance activities, inspections, accident monitoring and operation of equipment for the mitigation of severe accidents);
— Commercial off the shelf products;
— Mobile devices (e.g. hand-held, portable and wearable devices).

1.7. Additional guidance on HFE in the design and development of HMIs is available from organizations that develop industrial standards (see the Annex). Such standards provide much greater detail than is appropriate for IAEA safety standards. It is expected that this Safety Guide will be used in conjunction with such detailed industry standards.

OBJECTIVE

1.8. The objective of this Safety Guide is to provide a structured approach for, and guidance on, the application of HFE in the design and modification of HMIs in order to minimize the risk of human errors and optimize human performance to ensure safe operation of nuclear power plants.

1.9. The Safety Guide identifies the input information necessary to design and validate HMIs, which is the basis for human physical and cognitive processes.

SCOPE

1.10. This Safety Guide applies primarily to land based, stationary, commercial nuclear power plants. It could also be applied, using appropriate judgement, to other reactor types (e.g. small modular reactors), to determine the guidance that has to be considered in design.

1.11. The recommendations of this Safety Guide are to be applied in accordance with a graded approach, as set out in GSR Part 2 [4].

1.12. This Safety Guide applies to the application of HFE in the design, operation and maintenance of HMIs for new plants, as well as for modifications of HMIs of existing plants.

1.13. This Safety Guide is intended for use by organizations involved in the design, manufacture, construction, modification, maintenance, operation and decommissioning of nuclear power plants, in analysis, verification, validation, implementation and monitoring, and in the provision of technical support, as well as by regulatory bodies.

1.14. This Safety Guide does not address the application of HFE for purposes of nuclear security.

STRUCTURE

1.15. Section 2 provides guidance for the management of an HFE programme. Section 3 provides recommendations for review of operating experience; function analysis; function allocation; task analysis; analysis of staffing, organization and qualification; and treatment of important human tasks. Section 4 provides recommendations for the application of HFE in design. Section 5 provides guidance on the verification and validation of human factors in the design process. Section 6 provides recommendations on the implementation of the design of HMIs. Section 7 provides recommendations on human performance monitoring aspects of systems performance during plant operation. Section 8 provides recommendations on the application of HFE in design for computerized procedures. Section 9 provides recommendations on the integration of HFE into safety processes. Section 10 provides recommendations on the application of HFE in the specification and selection of products for subcontracted procurements. The Annex provides a list of international industrial standards for instrumentation

and control (I&C) and HFE that have a strong relationship with the major topical areas of this Safety Guide.

2. HUMAN FACTORS ENGINEERING PROGRAMME MANAGEMENT

GENERAL

2.1. GSR Part 2 [4] establishes requirements for the management system for all types of facility and activity.

2.2. Requirement 6 of GSR Part 2 [4] states: "**The management system shall integrate its elements, including safety, health, environmental, security, quality, human-and-organizational-factor, societal and economic elements, so that safety is not compromised.**"

2.3. Paragraph 4.24 of GSR Part 2 [4] states:

> "Competences to be sustained in-house by the organization shall include: competences for leadership at all management levels; competences for fostering and sustaining a strong safety culture; and expertise to understand technical, human and organizational aspects relating to the facility or the activity in order to ensure safety."

2.4. HFE should be applied to ensure the successful integration of human characteristics and capabilities with the design, commissioning, operation and maintenance of the nuclear power plant.

2.5. The integration of HFE into the design should be planned and documented, and should be an integral part of any nuclear power plant project.

2.6. An HFE programme should be developed and documented.

2.7. In the HFE programme, the nuclear power plant should be treated as a system comprising humans, technology and the organization, and the dynamic interactions within and among all relevant factors should be considered:

— Human factors (e.g. knowledge and expertise, cognition, performance expectations, motivation, stress, strength and body size);
— Technical factors (e.g. technology, including controls and displays, software, hardware, tools, equipment, plant design and plant processes);
— Organizational factors (e.g. management system, organizational structure, governance, resources, staffing levels, and the roles and responsibilities of managers and other plant personnel).

2.8. Humans, technology and the organization, as well as their interaction, should be considered in an integrated manner throughout the planning and execution of the HFE programme, during the design of the HMI and for resource allocation for all plant states.

2.9. In the HFE programme, a questioning and learning attitude should be applied to accepted design methods and solutions, with newly developed information, analysis methods, knowledge and features of new technology taken into account.

2.10. The HFE programme should be applied using the graded approach, as set out in GSR Part 2 [4], in order to identify the appropriate level of rigour, resources and detail to be applied.

2.11. The HFE programme should outline the HFE activities as well as the inputs to, and outputs from, these processes. HFE activities include analyses, design of the HMI, evaluations such as verification and validation, and monitoring of human performance (see para. 2.19).

2.12. The HFE programme should specify how HFE is integrated with other plant design or modification activities.

2.13. The HFE programme should identify the necessary coordination between personnel responsible for the HFE programme, project and design authorities, and personnel from other organizational units in the plant.

2.14. A process for communicating the outputs from analyses to the responsible engineering organizational units and for ensuring that the outputs have been addressed should be established and documented.

2.15. The HFE programme should identify the relevant organizational requirements and competence requirements (e.g. qualifications, skills, knowledge and training) for personnel performing HFE activities.

2.16. The HFE programme should provide a framework for documenting and tracking HFE related issues that are identified by the HFE processes.

2.17. The HFE programme should specify that the design team have a member or members with HFE expertise.

2.18. For the design of a new plant, the operating organization should assure itself that the intended plant design meets appropriate HFE standards and the recommendations of this Safety Guide.

THE HUMAN FACTORS ENGINEERING PROCESS MODEL

2.19. The overall HFE process can be divided into the following HFE activities:

— Programme management;
— Analysis;
— Design;
— Verification and validation;
— Implementation of the design;
— Human performance monitoring.

HUMAN FACTORS ENGINEERING ACTIVITIES WITHIN AN ENGINEERING PROJECT

2.20. HFE activities should be integrated into the basic stages of an engineering project as illustrated in Fig. 1.

2.21. The following should be considered as HFE inputs for the concept development stage:

— HFE programme management should identify a systematic, integrated HFE process, should outline responsibilities for HFE and should present expected design inputs and outputs for the HFE process.
— HFE programme management should establish a capable organizational unit with responsibility for human factors and with sufficient authority, at all hierarchical levels, to effect the necessary design changes to meet HFE expectations.

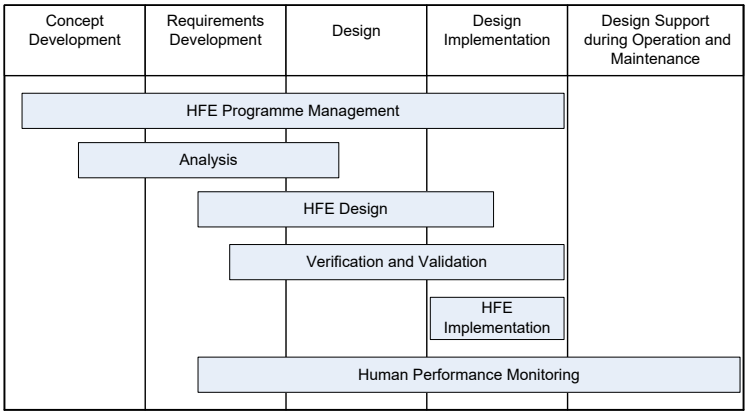

FIG. 1. An example of a generic engineering project, indicating when human factors engineering (HFE) activities are undertaken.

— HFE programme management should identify the most recent HFE relevant codes, standards, methodologies and guidelines applicable to the engineering project.
— HFE analyses should identify relevant operating experience (both positive and negative), with a focus on human performance issues and potential human errors and their mitigation.
— HFE analyses should provide inputs (such as operator needs and requirements) useful for defining and selecting relevant design choices.
— HFE analyses should be used to identify the organizational structure that frames the use of the HFE programme (i.e. the identification of users, their roles and responsibilities, required qualifications and regulatory requirements) and supports operation and maintenance.
— HFE analyses should provide a preliminary understanding of the allocation of functions and the human information requirements for monitoring and controlling, where applicable, the functions of systems in the plant.
— HFE analyses should provide insights and consideration of how operators are expected to respond in the presence of control system failures and HMI failures.

2.22. The following should be considered as HFE inputs for the requirements development stage:

— Results of the function analysis that identify the functional requirements for structures, systems and components.

— Results of task analyses that provide insight into:
  - What kind of alarms, information, procedures, controls and system feedback are necessary;
  - The possible sequence of tasks;
  - Potential human errors and considerations that impact human performance and provide error reducing and performance enhancing design features;
  - Safety significant, complex tasks that warrant detailed technical and HFE analyses;
  - Time constraints for significant tasks;
  - Specific knowledge, skills and abilities needed by personnel in order to perform their assigned task(s) and meet operational objectives;
  - Collaboration and coordination between individuals or groups that are necessary to support the task.
— Specific HFE design principles and HMI design guidelines for developing technical specifications for vendors and for incorporating them into HFE specifications for vendors.

2.23. The following should be considered as HFE inputs for the design stage:

— Updates to HFE requirements owing to design evolution or changes in standards;
— Specific HFE design principles and HMI design guidelines for the specification of plant and workspace design and layout, and HMI components and their architecture;
— Specific HFE design principles and HMI design guidelines for maintenance and testing;
— The potential impact of new or modified designs on human performance, and the development of procedures and training;
— Collection and analysis of user feedback through early HFE analyses in the form of usability testing and user reviews of prototypes and concepts;
— Insight into the scope, content and usability of operating procedures used to support the execution of safety critical tasks;
— Insight into the scope and content of training.

2.24. The following should be considered as HFE inputs for the design implementation stage:

— Verification of design implementation against previously identified HFE design principles and applicable HFE design codes, standards and guidelines;

— Verification of design implementation to ensure all information and controls required for carrying out tasks have been provided in the design;
— Validation in respect of human factors to ascertain the degree to which the HMI design and supporting mechanisms facilitate the achievement of safe operation of the plant;
— Confirmation of the feasibility of important human tasks in the probabilistic and deterministic safety analyses through validation in respect of human factors;
— Confirmation of the completion of HFE analyses and of HFE inputs into the design in accordance with the HFE programme and regulatory expectations.

2.25. Throughout the design stages, consideration should be given to the constraints of the technology being considered (e.g. availability, reliability, bandwidth, and the general acceptance and familiarity of the personnel with the technology). For example, although personnel accept the use of digital technology in everyday life, the designer may need to consider whether the use of virtual reality or augmented reality would cause difficulties for personnel.

2.26. Human performance monitoring in support of design should be conducted during the operation and maintenance stages in order to verify that analyses and assumptions from the design stage remain valid throughout the lifetime of the plant.

2.27. HFE activities supporting analyses, design, and verification and validation should be conducted in an iterative manner consistent with the overall design project.

2.28. HFE activities that support analyses, design, and verification and validation are often collaborative and should involve a multidisciplinary team with HFE expertise. In order to be properly addressed, the results of HFE analyses, design, and verification and validation activities should be communicated to other organizational units participating in the design.

2.29. The HMI and its functionality should be treated from the perspective of the HMI being part of an integrated whole and not merely an assembly of discrete controls, indicators and systems.

3. ANALYSIS

REVIEW OF OPERATING EXPERIENCE

3.1. Paragraph 5.28 of SSR-2/2 (Rev. 1) [2] states: "Events with significant implications for safety shall be investigated to identify their direct and root causes, including causes relating to equipment design, operation and maintenance, or to human and organizational factors."

3.2. Data and conclusions from event analyses should be used as HFE inputs for the design of a new plant or the modification of an existing plant.

3.3. The review of operating experience should provide information regarding current work practices for the following purposes: (i) to assess the potential impact of planned changes; (ii) to evaluate operational problems and difficulties in current designs that might need to be addressed during plant modernization and modifications to plant components; and (iii) to evaluate relevant industry experience with design options for I&C systems and HMI technology for their potential to improve plant efficiency and safety.

3.4. In the review of operating experience, both positive and negative aspects of performance and design should be analysed.

3.5. The review of operating experience should take into account:

- Applicable HFE related issues identified in the review of operating experience at the nuclear power plant;
- Insights from experience identified by plant personnel;
- Issues identified in the review of operating experience at other nuclear power plants and in other industries.

3.6. Operating experience data for any of the following should be taken into account:

- Minor problems (e.g. near misses or low level events) that are often precursors or contributors to more significant events;
- Adverse trends that could indicate a reduction in reliability;
- Data on root causes that could point to a need for improvements in design;
- Evidence of influences and trends in the organizational culture that could prove problematic for future operations;

— Corrective actions and their implementation;
— Recurring events;
— Reviews of maintenance practices;
— Industry communications on best practices.

3.7. IAEA Safety Standards Series No. SSG-50, Operating Experience Feedback for Nuclear Installations [7] provides recommendations for establishing, implementing, assessing and continuously improving an operating experience programme for nuclear installations to prevent or minimize the risk of future events by learning from events that have already occurred at the installation or elsewhere.

FUNCTION ANALYSIS

3.8. A function analysis should be conducted for all plant states to ensure that the functions necessary to accomplish safe operation of the nuclear power plant are sufficiently well defined and properly analysed.

3.9. The function analysis should provide a framework for understanding the role of personnel in controlling plant processes.

3.10. The function analysis should be used to identify the information (e.g. information on when a function is needed, available, operating, achieving its purpose or terminating) and controls that are necessary for the personnel to accomplish operational objectives.

3.11. The function analysis should provide time and performance requirements and constraints for performing the functions.

3.12. Human, technical and organizational factors should be considered when performing the function analysis.

3.13. The function analysis should be used to identify high level acceptance criteria associated with maintaining safe operation of the plant.

3.14. As part of the function analysis, the following should be analysed and documented:

— High level functions that ensure safe operation of the plant;

— Relationships (e.g. the plant configurations or success paths[2]) between high level functions and the plant systems responsible for performing those functions;
— The decomposition of high level functions into lower level functions that can be mapped to tasks to be performed by plant automation or by humans, or by humans and automation jointly;
— A framework for determining the roles and responsibilities of personnel and automation.

3.15. The combination of systems and processes used to achieve a high level function and the human actions required for the success path should be documented as part of the function analysis.

3.16. Dependencies that might exist among plant functions, plant systems and their support systems should be documented as part of the function analysis.

FUNCTION ALLOCATION

3.17. Allocation of functions should be conducted for all plant states to ensure that the functions necessary to accomplish safe operation of the nuclear power plant are sufficiently well defined and properly analysed.

3.18. The allocation of functions to personnel and automation should take into account human capabilities (e.g. the ability to improvise, flexibility, judgement and pattern detection) and machine strengths (e.g. rapidity and simultaneous processing of complex operations).

3.19. Human, technical and organizational factors should be considered when performing function allocation.

3.20. The design team should use knowledge of physical processes, current industry technology, operating experience, and human performance strengths and weaknesses to allocate functions to personnel and automation (e.g. hardware and software).

---

[2] A ‘success path’ is a set of selected structures, systems and components that provide high confidence that a nuclear power plant will successfully reach a safe state after an accident occurs.

3.21. Function allocation makes use of the function analysis of plant control systems and establishes the allocation of control processes, which might be assigned in the following ways:

- To personnel (e.g. manual control, with no automation).
- To automatic systems (e.g. fully automatic control and passive, self-controlling phenomena).
- To a combination of personnel and automation, for example:
  - Shared operation (i.e. the automatic operation of some aspects of a function, with other aspects performed manually);
  - Operation by consent or delegation (i.e. automation takes control of a function when personnel have given permission and the situation permits);
  - Operation by exception (i.e. automatic operation of a function, unless there are specific predefined situations or circumstances necessitating manual control).

3.22. In addition to consideration of human capabilities, when allocating functions, the designer should also take into account such factors as whether the technology is acceptable to personnel, timing capabilities associated with systems response, and considerations for defence in depth.

3.23. If the achievement of a control function requires the allocation of overlapping and redundant responsibilities to personnel and to automation (e.g. assigning personnel the responsibility of monitoring and maintaining supervisory control over automatic systems), this allocation should be documented.

3.24. The nature and scope of human tasks should be documented for all functions.

3.25. The allocation of functions should be analysed for various operational states and accident conditions.

3.26. Function analysis and the allocation of functions should take account of requirements associated with the implementation of severe accident management guidelines.

3.27. The allocation of functions should be traceable from the function to the associated system or component.

TASK ANALYSIS

3.28. The approach to task analysis should take into account the plant states and the groups of operating personnel (e.g. reactor operator, turbine operator, shift supervisor, field operator, safety engineer, and operation and maintenance staff) that are relevant to the task being analysed.

3.29. Human, technical and organizational factors (e.g. leadership, management and communication) should be considered when conducting task analysis.

3.30. Task analysis should be conducted to analyse and document the physical and cognitive activities associated with performing tasks assigned to personnel.

3.31. Task analysis should include the context of the task from the standpoint of the user who will accomplish the task.

3.32. The role and activities of individuals in a nuclear power plant are wide ranging, and, therefore, the scope of analysis should be justified and will often include:

— Tasks that are performed in different locations (e.g. control room, supplementary control room, local control stations, emergency response facilities);
— Tasks that differ depending on the plant state;
— Tasks that require individual work and/or cooperation or exchanges between different organizational units (e.g. operations, maintenance, procedures development and computer systems engineering) and interested parties;
— Tasks that sometimes have to be performed under time pressure or harsh environmental conditions and contexts, or that are safety critical and rarely performed.

3.33. Risk and safety aspects should also be considered when identifying the tasks to be included in the task analysis, which could include:

— Tasks posing an occupational risk to personnel;
— Tasks credited in the safety analysis;
— Tasks identified from operating experience as challenging or prone to error;
— Tasks identified as difficult by operating personnel and for which no plans have been made to automate that task;
— Tasks that are critical for maintaining the plant in a safe state or restoring it to a safe state following an event.

3.34. Responses to alarms, and surveillance and maintenance tasks directed from the control room by operators should also be analysed.

3.35. The results from task analysis should serve to identify:

— The expected human tasks and the potential human errors that have an impact on safety;
— The expectations regarding how each task will be conducted, the expected task outcomes, and estimates of the reliability of human performance for the task;
— The means for error prevention in place for safety critical tasks;
— The safety functions impacted and the initiating conditions and terminating conditions for each task;
— The sequence for implementing tasks and subtasks;
— The personnel needs (e.g. organizational aspects, staffing, qualification and training), the equipment needs (e.g. HMI elements, special tools and protective clothing) and the documentation needs (e.g. procedures, processes and instructions);
— The human performance requirements and constraints (e.g. time, precision and independent verification);
— Required communication systems and access to those systems.

3.36. To conduct a task analysis, information from the following sources should be considered:

— Documentation (supplier documentation, technical specifications, existing procedures, manuals and training materials);
— Knowledgeable personnel from the design team, operating personnel who have gained operating experience in similar plants, interested parties and experts from other industries;
— Walkthrough and ‘talkthrough’ to analyse tasks performed by a predecessor system and tasks from similar plants, as well as the tasks associated with the system being developed;
— Data from the review of operating experience (with account taken of differences from the reference design);
— Data from the customer’s requirements;
— Data from other analyses that are inputs to the HFE design process (e.g. function analysis and allocation, and treatment of important human tasks);
— Data from simulator studies;
— International HFE standards (see also the Annex).

3.37. The choice of technique(s) adopted for conducting the task analysis should be justified.

3.38. The impact of performance requirements for the task on human reliability should be evaluated.

3.39. The process for collecting, tabulating and analysing the inputs for the task analysis should be documented.

3.40. Task analysis is a collaborative activity and should involve a multidisciplinary team with HFE expertise and operations expertise.

3.41. The results of the task analysis should be communicated to the other organizational units participating in the design for their consideration.

3.42. The results of the task analysis can be directly used to support the assessment of human errors.

3.43. Task analysis should particularly be performed for tasks in which cognitive processes, such as decision making, problem solving, memory, attention and judgement, are important.

3.44. A tabletop analysis of documentation (e.g. procedures) alone might not be sufficient for determining whether a task or tasks can be performed. Input from simulations supported by mock-ups, plant walkdowns, partial task simulators or full scope simulators may be performed to confirm the feasibility of the tasks in real scenarios.

3.45. Task analysis should contain a means of error classification that, at a minimum, captures the potential errors of omission and errors of commission, including decision errors and communication errors, associated with each task.

ANALYSIS OF STAFFING, ORGANIZATION AND QUALIFICATION

3.46. Staffing, the organizational structure and the qualifications of personnel should be analysed for their impact on important human tasks to determine the required number of personnel, organizational interactions and qualifications of personnel.

3.47. In the case of modifications to existing plants or for new plants, an analysis of staffing, organization and qualification should be conducted that takes into account any change in relation to reference plants that could impact:

— The safe completion of human tasks;
— The workload of the personnel;
— The ability to align the contribution of each team member with a team's task;
— The independence and cooperation of the individuals responsible for checking the progress of tasks (e.g. checking actions taken in the control room and locally by the operators);
— The perception of the task and its benefits, and its acceptance by the personnel.

3.48. Staffing, organization and qualification analysis should cover all the teams that carry out tasks with an impact on safety (see paras 3.28–3.45 on task analysis). This includes all teams of operating personnel, service support teams, and emergency preparedness and response teams. The analysis should identify and evaluate the needs of these teams in terms of staffing, organization and qualification.

3.49. Staffing, organization and qualification analysis should evaluate the impacts of organizational and technological differences with respect to the reference plant.

3.50. The inputs to the staffing, organization and qualification analysis should include:

— Concept of operations in operational states and accident conditions;
— Design requirements;
— Task requirements;
— Regulatory requirements;
— Operating experience;
— Treatment of important human tasks (e.g. treatment of important human tasks might determine that a two person rule needs to be in effect to ensure reliable completion of certain tasks).

3.51. Task analysis should be used in support of defining roles, requirements and responsibilities, and required outputs of teams.

3.52. The following should be ensured when assigning individual tasks to team members:

— The tasks assigned to each member should be clearly described.
— The basis for task distribution should be determined and justified.
— The workload of each team member should be reasonable in all operational states and accident conditions.
— The impact on human performance should be taken into account when distributing the tasks between teams working during the day and teams working at night.
— The tasks required in various operating situations should be assigned to team members in a manner that ensures continuity of responsibilities and maintains individual and team situation awareness.

3.53. Any reduction of staffing should be evaluated for its potential impact on safety by modelling, analysis or full scope simulator tests.

TREATMENT OF IMPORTANT HUMAN TASKS

3.54. Important human tasks and actions should be identified from probabilistic or deterministic safety analysis.

3.55. The underlying approach to determining important human tasks should take into account both operational states and responses in accident conditions.

3.56. An analysis supporting the application of HFE in design can take the form of qualitative and/or quantitative analysis.

3.57. At a minimum, important human tasks and actions credited in the safety analysis, including relevant factors that impact performance, should be analysed, and it should be confirmed that the design solution is such that safety requirements relating to human performance will be met.

3.58. Irrespective of the approach taken to identifying important human tasks, the design, procedures, training, staffing levels and concept of operations should support the execution of important human decisions and actions.

3.59. Plant modifications might alter the manner in which important human tasks are executed. For all plant modifications, it should be assessed whether associated important human tasks can still be reliably executed.

4. DESIGN

GENERAL

4.1. Requirement 32 of SSR-2/1 (Rev. 1) [1] states: "**Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.**"

4.2. Paragraph 5.55 of SSR-2/1 (Rev. 1) [1] states:

> "The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states."

4.3. Paragraph 5.56 of SSR-2/1 (Rev. 1) [1] states:

> "The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make decisions to act shall be simply and unambiguously presented."

4.4. The means for interaction between humans and machines should be designed through a structured methodology that permits, from conceptual design, the identification and selection of candidate HMI approaches, the definition of a detailed design, and the performance of HMI tests and evaluations, when necessary.

4.5. The concept of defence in depth should be applied in the design of the HMI to ensure that if a failure were to occur, it would be detected and compensated for, or corrected by, appropriate measures.

4.6. The design should apply a human centred approach in which the equipment and systems are considered from the perspectives of the personnel who will carry out the associated functions and tasks.

4.7. Human aspects, technology (both hardware and software), the working environment, and the control, operational and management strategies to be applied should be taken into account at all stages of the design process (in accordance with an integrated, systemic approach).

4.8. The designer should consider how information relayed by the HMI will be communicated, exchanged and used by different groups (e.g. staff in the main control room and in emergency response facilities).

4.9. The designer should take into account the necessary constraints and ensure that there is flexibility in the design to adopt different control and operational strategies for the different plant states and plant operating modes.

4.10. Design considerations should provide for operator and organizational resilience by examining:

— Whether automatic actions are properly allocated for response to a postulated initiating event;
— Whether the HMI can support anticipation of, and response to, an unexpected event;
— Whether the HMI provides information on incremental changes in anticipation of sudden disruptions or fault conditions (e.g. use of predictive displays);
— Whether provisions and locations for additional tools and equipment are available;
— Whether implementation by the operating organization of 'stress tests' of the response of plant systems to severe accidents provides insights for how operators might be able to use equipment for purposes other than the original intent in order to protect fission product boundaries;
— Whether different operational strategies might have to be adopted in order to achieve a safe state as an event unfolds;
— Whether equipment could be used out of its design intent to support the adoption of a different strategy (e.g. use of the fire protection system for heat removal).

Human–machine interface design inputs

4.11. The requirements to be considered in the HMI design should be identified through the following analyses, performed at earlier stages of the design process (see Section 3):

— Operating experience review;
— Function analysis and function allocation;
— Task analysis;
— Analysis of staffing, organization and qualifications;
— Treatment of important human tasks.

4.12. Important inputs to be considered in the HMI design are:

— Constraints imposed by the overall I&C system (e.g. constraints on the information that can be presented due to the availability of sensor data);
— The physical environment in which the HMI is to be deployed;
— Cognitive limitations and cognitive strengths of the users;
— The knowledge, skills and abilities of personnel, including personnel from various occupational groups;
— Applicable regulatory requirements.

4.13. The HMI design should support the roles of plant operators, and should take into account the levels of automation identified in the processes of function analysis and function allocation.

4.14. Results from the task analysis should provide input to the HMI design as follows:

— Tasks necessary to control the plant during a range of plant states, from normal operation to accident conditions;
— Detailed I&C requirements (e.g. requirements for display range, precision, accuracy and units of measurement);
— Requirements relating to aspects that support tasks, including habitability (e.g. lighting and ventilation requirements).

4.15. Results from staffing and qualifications analyses should provide inputs to the HMI design for decisions on the layout of the overall control room, and the allocation of controls and displays to individual consoles, panels and workstations.

4.16. Specific guidance on the application of HFE in design should be documented and used in designing the features of the HMI, their layout and the environments in which the HMI will be deployed.

4.17. This guidance should specify the detailed design criteria for the HMI elements. If the HMI in an existing plant undergoes modernization, the guidance

should be evaluated for any necessary revisions based on both the HMI modernization and the concept of operations.

4.18. This guidance should be developed from generic HFE guidance and analyses relating to the HMI design. It should specifically reflect the design decisions taken in addressing specific aspects of the HMI design.

Detailed design of the human–machine interface and its integration into the overall design of the plant

4.19. The HMI should provide operators with the information necessary to detect changes in plant status, to diagnose the situation, to take action and to verify manual or automatic actions.

4.20. The HMI design should support human performance under a full range of environmental conditions, such as loss of lighting, smoke, high radiation levels, flooding, steam ingress and limited ventilation.

4.21. All aspects of the HMI (including controls, display arrangements and coding techniques) should be consistent with the mental models used by operators and with established conventions.

4.22. Information should be presented in a manner that optimizes the understanding of operators of the status of the plant and the activities necessary to control the plant.

4.23. The operation and appearance of the HMI should be consistent across information and I&C locations.

4.24. To the extent possible, the HMI should be designed to prevent and detect operator errors, in particular in cases in which an action might be taken in an incorrect context or with an inappropriate plant configuration. This includes design to ensure the validation of set point changes to control systems, monitoring systems and protection systems.

4.25. The HMI design should provide enough information to operators to support decision making in cases in which erroneous information is presented.

4.26. To the extent possible, information flow diagrams and control actions should complement the information processing capabilities and the performance of operators.

4.27. The design of the HMI:

— Should, as far as practicable, accommodate the different roles and responsibilities of various types of operating personnel expected to interact with the plant;
— Should be designed with primary attention given to the role of the operator who is responsible for the safe operation of the equipment;
— Should support the development of a common situation awareness on the part of the control room staff (e.g. by means of large wall-mounted plant status displays);
— Should provide an effective overview of the plant status;
— Should, as far as practicable, apply the simplest design from the users' perspective that is consistent with function and task requirements;
— Should present information such that it can be rapidly recognized and understood by operators (e.g. taking into account knowledge about human information processing and visual attention);
— Should accommodate failure of analogue and digital displays without significant interruption of control actions;
— Should reflect consideration of human cognition, physiological characteristics, characteristics of human motor control and human body sizes.

4.28. The HMI should provide simple, comprehensible notifications of detectable operator errors, and should make available simple, effective methods for recovery.

4.29. The HMI procedures and the training programme should be designed and compared to ensure consistency with each other.

4.30. The use of a single language and compatible script for all descriptive identification and labels should be considered.

4.31. The HMI design should allow for inspection, maintenance, testing and repair of the HMI without interfering with other plant control activities.

4.32. The HMI design should support the performance of tasks by the personnel under conditions of minimum, typical and optimal staffing.

4.33. In the case that the HMI is modified, both the modified HMI and any new HMI should be designed:

— To be consistent with the design guidance used for the existing HMI, so that personnel have a similar interface across new and old equipment;
— To be consistent, as far as possible, with users' existing strategies for gathering and processing information, and executing actions identified in the task analysis.

4.34. If the HMI is modified, any reduction of information displays should be justified, reviewed and agreed upon among design engineers, human factors engineers and operators.

4.35. The HMI design of local control stations should be consistent with the HMI design in the control room.

4.36. The HMI design required for the supervisory control of safety systems should apply the concept of defence in depth.

4.37. A description should be provided of how the HMI presents the controls, displays and alarms that ensure the correct and reliable performance of the identified important human tasks.

4.38. The HMI design should take into account the necessary compensatory actions and supporting procedures to ensure that the personnel effectively manage any degraded I&C functions and HMI conditions, and provide for the transition to backup systems.

Tests and evaluations of the human–machine interface

4.39. Usability tests of concepts and detailed design features should be conducted during the process of developing the HMI.

4.40. 'Trade-off' evaluations are comparisons between design options, based on aspects of human performance that are important to successful task performance and on other design considerations. Such trade-off evaluations should consider:

— Requirements for human tasks;
— Human performance capabilities and limitations;
— Performance requirements for the HMI;
— Inspection and testing needs;

— Maintenance demands;
— The use of proven technology and operating experience with predecessor designs.

4.41. Usability and performance tests involve assessing HMI performance, including user opinions, to evaluate design options and design acceptability.

Design of human–machine interface controls

4.42. If a control can be accessed from more than one location, such as from the control room, from the supplementary control room or from equipment located in the plant, protective measures should be applied to ensure its coordinated use among multiple operators.

4.43. HMI controls may be implemented as 'soft' controls (see paras 4.50–4.61) for multiplexed control devices or dedicated control devices, or for a combination thereof.

4.44. Analogue control devices (e.g. push buttons, rotary switches, slides, toggle switches and rocker switches) are suitable for controls that are in constant use (e.g. an electrical output) and for controls whose immediate accessibility and reliability are of prime importance (e.g. an emergency trip button).

4.45. Controls should provide optical and/or acoustic feedback within an adequate time to indicate that the system has received a control input.

4.46. The use of controls should be accompanied by feedback for the operators to indicate the process of data entry (e.g. adjustment of the set point limit) and to acknowledge the completion of data entry.

4.47. The HMI should ensure that the likelihood of unintended actuation is minimized by requiring deliberate action for the execution of actions that can have negative consequences (e.g. a confirmation button and a plastic cover over the switch).

4.48. Means to prevent erroneous activation of analogue controls should include:

— Locating controls at proper positions;
— The use of protective structures;
— A demand for a second confirmatory action;

— The use of interlocks or permissive signals, with proper assignment of priorities;
— The proper selection of physical characteristics, such as size, operating pressure or force, and tactile, optical and/or acoustic feedback.

4.49. To minimize operator errors, control movements should conform to routine actions (e.g. they should meet users' expectation) and should be compatible with the attributes of the controlled variable.

Design considerations for soft controls

4.50. Soft controls are implemented using video display units together with a pointing device (e.g. a mouse, track ball, light pen or touch capability), or a combination of a video display unit with a set of dedicated controls.

4.51. Information displays important to operator performance that use soft controls should include the means for selecting the components to be controlled, as well as the display areas where input is entered and the formats used for entering data.

4.52. Soft controls should be used for interactions such as selecting a plant variable or component to be controlled, providing the control input and monitoring the system's response.

4.53. Soft controls should provide display devices:

— To allow access to individual components, when necessary;
— To allow access to information about the status of each component;
— To control the relationship to other components.

4.54. 'Selection displays' show a set of components or variables to be controlled. Components and variables within a selection display should be visually distinct, clearly laid out and uniquely labelled to support correct selection.

4.55. Soft controls should be designed so that operators can, at a glance, distinguish options by such characteristics as context, visually distinct formats, separation, input fields and selectable components.

4.56. Input formats commonly used with soft controls are discrete control interfaces, soft sliders and arrow buttons. Input formats for entering data should be provided in the soft controls.

4.57. Cursors should have a distinctive appearance and their movement should have a sensitivity compatible with the required tasks and operators' skills. Cursor movement should conform to characteristics relating to the reach, vision and comfort of operators, allowing both fast movement and accurate placement.

4.58. Actions that control navigation within the HMI should be distinguished from actions that control the plant, such as turning off or on a pump from the computer screen.

4.59. Control entries for any particular action should offer the operator only the options and controls that are available for selection. The options should be listed in a menu added to the working display without requiring the operator to memorize them or to access a separate menu display.

4.60. Soft control menus should be designed consistently and their option lists should also be consistent in wording throughout the HMI.

4.61. In order to avoid errors when executing a command, the sequence of control should comprise selection of the control, selection of the command and validation of the command.

Application of human factors engineering in the design of workstations

4.62. The design of workstations should take into account characteristics relating to the reach, vision and comfort of operators, such as:

— Workstation height;
— Inclination of benchboards, angle and depth of consoles, and workstations that can be adjusted for sitting and standing;
— Control device location;
— Display device location;
— Layout of control and display devices at a console or workstation;
— Size and legibility of text and graphics;
— Space for legs and feet.

4.63. The height of a console should allow operators to see over its top (e.g. to see shared displays and other operators).

4.64. The position of alarm panels should be such that they are visible from the operating area of the main control room and are at a convenient height for operator visibility and for legibility.

4.65. Frequently used controls should be within reach of operators, and the related indicators and displays should be readable from the operator's position.

4.66. Functions and process operations should be grouped into functional groups in accordance with their characteristics.

4.67. Functional groups should be organized by function, by sequence of use, by frequency of use, by priority, by operating procedures or by a system with a mimic display[3] arrangement.

4.68. Functionally related controls and displays should be distinguishable from controls and displays of other functional groups.

4.69. A mirror image layout of panels, controls and indicators should be avoided in order to prevent 'left–right' confusion on the part of operators.

4.70. Controls, displays and other items of equipment located at workstations should be appropriately and clearly labelled to facilitate prompt and accurate human performance.

4.71. A hierarchical labelling scheme should be used to reduce confusion, search time and redundancy. Major labels should be used to identify major systems or workstations, subordinate labels should be used to identify subsystems or functional groups, and component labels should be used to identify each workstation element.

4.72. The label should describe the function of equipment items, and the symbols used should be unique and distinguishable from each other.

4.73. Labels should be consistent within and across panels in their use of words, acronyms, abbreviations, and system and component numbers, and there should be no mismatch between the nomenclature used in procedures and that printed on the labels.

[3] A 'mimic display' is an arrangement on the display panel that simulates the physical layout of the plant.

4.74. The design of workstations should take into account the test and maintenance operations that might have to be performed at the workstation. This consideration should include:

— Access to the components on the panels for repair, removal or replacement;
— Separation of controls and displays used only for testing and maintenance from those used for operations;
— Contingency space for special test equipment or for access for repairs.

APPLICATION OF HUMAN FACTORS ENGINEERING IN DESIGN FOR ACCESSIBILITY AND THE WORKING ENVIRONMENT

4.75. Paragraph 5.60 of SSR-2/1 (Rev. 1) [1] states:

> "The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel."

4.76. Paragraph 5.61 of SSR-2/1 (Rev. 1) [1] states: "The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts."

4.77. In areas in which operating personnel are expected to monitor and control plant systems, the necessary provisions should be made to ensure suitable conditions in the working environment and to protect against hazardous conditions.

4.78. Aspects of the working environment that should be considered include lighting, temperature, humidity, noise and vibration.

4.79. Hazards that should be considered include radiation, smoke and toxic substances in the atmosphere.

4.80. One way of ensuring suitable means of access is to provide qualified routes that are protected against potential internal hazards and external hazards to supplementary control points and other field locations where operator actions are expected to be taken.

MAIN CONTROL ROOM

4.81. Requirement 65 of SSR-2/1 (Rev. 1) [1] states:

> "**A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions.**"

4.82. Paragraph 5.57 of SSR-2/1 (Rev. 1) [1] states:

> "The operator shall be provided with the necessary information:
>
> (a) To assess the general state of the plant in any condition;
> (b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);
> (c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;
> (d) To determine both the need for and the time for manual initiation of the specified safety actions."

4.83. Paragraph 6.39 of SSR-2/1 (Rev. 1) [1] states:

> "Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, releases of radioactive material, fire, or explosive or toxic gases."

Human–machine interface design for the main control room

4.84. The design of the main control room should be consistent with the concept of operations, which describes how the plant will be operated in all plant states.

4.85. The HMI in the main control room should be designed giving due consideration to:

— Operating goals and objectives, including safe operation;

— The organization of the HMI into workstations (e.g. consoles and panels);
— The arrangement of workstations and supporting equipment in the main control room.

4.86. The HMI of displays should enable the operators to:

— Recognize the actions being taken by the reactor protection system and other automatic systems;
— Analyse the cause of disturbances and follow their course;
— Perform any necessary manual counteractions.

4.87. The design of the main control room should consider the display options that would provide a high level summary of plant status and would support the cooperation of operators on shared tasks and their awareness of one another's activities.

4.88. Display devices should be provided in the main control room in order to allow operators and supervisors to monitor all safety functions, including the status of the plant, its safety status and trends in key plant parameters.

4.89. HMI elements and codes (e.g. colours, shapes, lines, labels, acronyms and abbreviations) should be identifiable and legible from the maximum viewing distance for each specific task under minimal ambient lighting conditions.

4.90. The display system should communicate the intended information to the operator without ambiguity or loss of meaning, and without unnecessary time delay or latency.

4.91. The display capability should allow operators to quickly assess the status of individual HMI elements and their relationship with other HMI elements.

4.92. Numerical values should be displayed only to the level of significance required of the data for operation, even when more precise individual input data are available.

4.93. The response time of display systems should be consistent with operational requirements.

4.94. When several operators are required to interact with the system simultaneously, control entries by one operator should not interfere with other control entries of higher priority.

4.95. The HMI design should take into account where common or coordinated actions are to be made by the operators.

4.96. Information from the HMI should allow operators to immediately assess the overall plant status and to detect conditions that require attention without the need to perform additional complex tasks.

4.97. Information shown on video display units should be clearly understandable in any operating condition.

4.98. Symbols used in the display system should be standardized.

4.99. A display feature should be provided to indicate to the operator that the system is operating properly (or that a system failure has occurred).

4.100. Where overload of the display system or other system conditions could result in a processing delay, the system should acknowledge the data entry and should provide the operators with an indication of the delay and of the completion of the processing.

4.101. HMIs for real time tasks requiring a fast response from operators should require only limited operator actions. For example, the travel distance for cursors across and between display pages, the scanning time and the number of windows on a display should be limited.

4.102. User assistance should be provided by the video display unit systems. Such assistance should include, when necessary, advisory messages, error messages, confirmation messages and validation systems.

4.103. Operators should be able to request guidance regarding requirements for entering commands (e.g. the required syntax, parameters and options).

4.104. The organization of the display network should reflect an obvious logic based on task requirements and should be readily understood by operators.

4.105. The display screen should be organized such that the location of various HMI functions (e.g. the data display zone, the control zone and the message zone) is standardized from one display to another.

4.106. The HMI display system should clearly indicate which items are available for selection. When the operator performs an operation on a selected display item, this item should be highlighted in order to avoid errors.

4.107. The HMI should be user friendly and should not require the operator to memorize special codes or sequences to perform actions.

4.108. Large screen displays may be used to enhance the performance of operators by enabling access to a common view of plant information or a means of sharing information.

Layout of the main control room

4.109. The main control room should have sufficient space to allow the main control room staff to perform all necessary actions, while minimizing the need for operator movement in abnormal and accident conditions.

4.110. The main control room staffing and task assignments should be such that controls, displays and other necessary equipment are fully and rapidly accessible for all modes of operation.

4.111. The layout of workstations and consoles in the main control room:

- Should permit full view of all control and display panels (including alarm displays);
- Should facilitate verbal communication from operators at the workstations to any point in the main operating area;
- Should permit access to workstations without the need to overcome obstacles;
- Should permit efficient, unobstructed movement and communication.

4.112. A storage space for procedures and other documents should be provided in the main control room. Such storage spaces should allow for easy access and easy extraction of documents.

4.113. A storage space for emergency equipment that control room staff might require during an accident should be provided. Such storage spaces should allow for easy access.

Habitability considerations

4.114. The environment of the main control room should be such that the main control room staff are able to perform their tasks without discomfort, excessive stress or physical hazard.

4.115. The design of the workspaces in the main control room should consider environmental factors that could have an important effect on the performance of the personnel, such as thermal comfort, adequate illumination including in the event of an emergency, auditory environments that promote clear verbal communication, and a suitable layout.

4.116. The control room should contain sufficient facilities and supplies to ensure comfortable long term occupation during a response to an accident.

4.117. The control room design should include an assessment of, and protection against, missiles originating from outside the control room. Guidance on protection of the control room from missiles is provided in IAEA Safety Standards Series No. NS-G-1.11, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants [8].

Design of the safety parameter display system

4.118. A safety parameter display system should be provided to aid, during an accident, the main control room staff in determining the safety status of the plant and in evaluating whether conditions require corrective action by operators to avoid a degraded reactor core or release of radioactive material.

4.119. HFE should be applied in the design of the safety parameter display system in order to enhance the functional effectiveness of the main control room staff.

4.120. The safety parameter display system should provide information on the critical safety functions associated with the plant.

4.121. The safety parameter display system should be placed in a location convenient for the main control room staff and should provide continuous display information from which the plant status can be readily and reliably assessed.

4.122. The safety parameter display system should be designed to bring together a minimum set of plant parameters from which the operator can assess

the plant status without the need to survey all information on display in the main control room.

4.123. The display devices for the safety parameter display system might include analogue devices and computer based devices. Analogue display devices could include meters, light indicators, numeric readouts and plotters. Computer based display devices could include flat panel devices and large screen devices.

4.124. The display devices used for the safety parameter display system should conform to the general design guidelines for the main control room HMI.

4.125. The safety parameter display system should be consistent and compatible with other displays and devices of the HMI in terms of presenting and coding information.

SUPPLEMENTARY CONTROL ROOM

4.126. Requirement 66 of SSR-2/1 (Rev. 1) [1] states:

> "**Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.**"

4.127. The HMI design process for the supplementary control room should be performed in parallel with the design process for the main control room, using similar procedures, criteria and methods.

4.128. The HMI design of the supplementary control room should take into account HFE principles and human characteristics of personnel under emergency conditions, with particular consideration given to the need to take immediate actions.

4.129. Means should be provided to ensure habitability of the supplementary control room, including in the case that long term occupation of the supplementary

control room is required (e.g. equipping ventilation systems with a backup power supply and with filters such as iodine filters).

4.130. The design of the workspaces in the supplementary control room should consider environmental factors that could have an important effect on the performance of the personnel, such as thermal comfort, adequate illumination including in the event of an emergency, auditory environments that promote clear verbal communication, and a suitable layout.

4.131. Computer based information or controls used in the supplementary control room should function in a manner that closely matches or, preferably, is identical to that of similar controls and indications in the main control room.

4.132. The HMI for displays and controls in the supplementary control room should be similar to that in the main control room to allow for an easy transfer for operators, and should be arranged according to its functions in order to minimize the likelihood of human errors.

4.133. A procedure should be established for the transfer of command, controls and communications from the main control room to the supplementary control room.

4.134. Means should be provided for communication between the supplementary control room and local control points, and with the plant management, external crisis management teams and the technical support centre.

EMERGENCY RESPONSE FACILITIES ON THE SITE

4.135. HFE should be applied in the design of emergency response facilities[4] on the site. The design should provide for an optimal layout of individual workplaces, and the data and information necessary to perform the activities required for the implementation of accident management strategies.

[4] Emergency response facilities are addressed in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [9]. For nuclear power plants, emergency response facilities (which are separate from the control room and the supplementary control room) include the technical support centre, the operational support centre and the emergency centre.

4.136. Displays in emergency response facilities supporting situation awareness should be designed through application of accepted HFE methods and principles. Factors to be considered include illumination, size, geometry, display and control layouts, availability of content, suitability of format and standardization of the displays. Fundamental consideration should be given to the task to be performed with the information provided by the display.

4.137. Reviews of operating experience, including emergency exercises, combined with function analysis and task analysis should provide the bases for identifying the human performance related requirements for accident monitoring and operation of equipment for the mitigation of the consequences of a severe accident.

4.138. Consideration should be given to resource allocation strategies (e.g. staffing), the physical conditions of the plant (e.g. power supply, accessibility, and environmental and radiological conditions), exacerbating factors such as weather conditions (extreme heat, cold or precipitation), and technology selection in relation to human performance under emergency conditions.

4.139. HFE aspects should be considered when personnel are required to operate non-permanent equipment credited in the safety analysis for severe accident management. This includes safe access to local controls to enable the safe use of non-permanent equipment. Typical examples of local controls include local control panels, connection points, switches and terminals that (i) enable the connection of non-permanent equipment or (ii) enable the operation of equipment (e.g. pumps) for which non-permanent equipment provides electric power.

4.140. Consideration should be given to the range of internal and external interactions of individuals and interested parties at all levels with the on-site and off-site emergency response organizations under emergency conditions.

4.141. Consideration should be given to the levels of stress and workload that can exist during emergency response operations.

4.142. The technical support centre staff should be trained in the identification and use of the instruments to support the implementation of severe accident management guidelines. More detailed recommendations for the development and implementation of severe accident management guidelines are provided in IAEA Safety Standards Series No. SSG-54, Accident Management Programmes for Nuclear Power Plants [10].

ALARM MANAGEMENT

4.143. Paragraph 5.66 of SSR-2/1 (Rev. 1) [1] states: “Suitable alarm systems and means of communication shall be provided so that all persons present at the nuclear power plant and on the site can be given warnings and instructions, in operational states and in accident conditions.”

4.144. Alarms or other devices indicate deviations of conditions from those associated with normal operation. When this occurs, the operators should be provided with the information necessary to:

— Identify the actions being taken by automatic systems;
— Perform any necessary manual counteractions;
— Follow the course of the plant’s behaviour or response.

4.145. Alarms should provide information about abnormal conditions such as:

— Parameter deviations or rate of change deviations from control or protection set points;
— Equipment failures, anomalies or discrepancies;
— Incomplete or failed automatic actions.

4.146. Conditions that do not require any operator action should not result in alarms. Data derived from planned situations that do not indicate abnormalities but are rather messages from an expected system response should be included as status information.

4.147. All alarms should be documented and under configuration control.

4.148. The alarm system should have sufficient coverage to be capable of generating alarms for operational states and accident conditions.

4.149. Paragraph 7.9 of SSR-2/2 (Rev. 1) [2] requires that the number of alarms be minimized for any analysed operational state, outage or accident condition of the plant, in order to prevent unnecessary or meaningless alarms that could result in alarm overload.

Alarm generation

4.150. The alarm system should be capable of generating alarms from the following sources:

— Digital signals;
— Analogue signals;
— Calculated, synthesized or grouped signals from direct inputs or derived from other systems.

4.151. Alarms based on analogue and digital signals should be configurable. The alarm state can be selected among the different states of the signal (e.g. on/off, open/closed and tripped/untripped).

4.152. The generated alarms should support an alarm hierarchy that is consistent with the architecture of structures, systems and components in the plant.

4.153. Alarms should be context aware (e.g. pump low flow alarms should be generated upon real low flow conditions and not during pump startups).

Alarm validation

4.154. Sensor and input signals for alarm generation should be validated to prevent the generation of unnecessary momentary or chattering alarms.

4.155. Alarm systems should be able to automatically reduce the number of alarms being generated at any one time.

4.156. Alarm inhibition takes inactive alarms out of service by disabling alarm generation, normally during testing, maintenance or repair of the associated equipment. Alarm systems should support alarm inhibition to avoid alarms occurring as nuisances or becoming standing alarms.

4.157. HFE analysis and validation should be used to determine whether one alarm is masking the occurrence of another alarm or other alarms.

4.158. Alarm systems should support the prioritization of alarms to determine their relative importance.

Alarm processing

4.159. The alarm system should support user defined generation of alarms. Operators should be able to select one high or one low alarm limit for analogue variables or one state among the possible alarm states for discrete variables.

4.160. Alarm systems should be able to apply event based and significance based alarm suppression techniques, as follows, at different hierarchy levels:

— Event based reduction techniques filter or suppress alarms generated as a consequence of the failure of a support system or item of equipment, or as a consequence of a plant event;
— Significance based reduction techniques suppress lower priority alarms in situations with alarm overload.

4.161. Alarm filtering or suppression, whether automatic or operator initiated, should be used to avoid overloading the operator, but should not suppress necessary information.

Alarm annunciation and control

4.162. The alarm system should provide visual indications when any alarm condition appears or clears. Visual indications could include:

— Flashing, initiated when the alarm condition appears or clears, and terminated after acknowledgement or reset, respectively. Grouped alarms should reflash when any new sub-alarm appears after another sub-alarm has already been set off and has been acknowledged.
— Colour coding: alarms can light with different colours depending on the alarm priority and on the alarm state. Other display coding methods may be used.

4.163. The alarm system should provide auditory indications when any alarm condition appears or clears.

4.164. Means for silencing audible signals should be provided in order to avoid auditory overload and to facilitate the recognition of new alarms that might occur subsequently.

4.165. Means should be provided that permit the operator to acknowledge the alarms, either singly or in groups, in a timely manner.

Alarm presentation

4.166. The ‘dark board’ criterion consists of minimizing the number of alarms presented during normal operation without challenging plant safety.

4.167. Alarm processing should follow the dark board criterion at full power and for other conditions of normal operation.

4.168. Alarm presentation should be based on the following different types of display:

— Spatially dedicated, continuously visible displays (e.g. analogue tile panels or arrays of visual display units with continuously visible tile-like panels, or continuously visible mimic displays with integrated alarms);
— Alarm message list displays (e.g. text messages presented on visual display unit screens);
— Alarms integrated into graphic displays (e.g. mimic displays or soft control displays);
— Individual alarm information displays;
— Mixed displays (i.e. a combination of the other types of display).

4.169. Information about alarm state changes and new alarms should be presented and managed separately.

4.170. Alarm messages should be simple, unambiguous and standardized.

4.171. Alarm messages should contain all the information that the operators need to respond to the alarms effectively, such as alarm sources, priorities, descriptions, set points and parameter values, and references to alarm response procedures and associated displays.

4.172. Operators should be able to sort alarm messages on demand. The alarm system could provide lists of alarms organized by:

— Chronological order;
— Priority level;
— Alarm state;
— Alarm message;
— Any other logical order.

4.173. Alarms should be integrated into graphic displays, especially when it is beneficial to show the relationship of the alarm to related systems, functions, equipment or components.

4.174. Individual alarm information displays should be used to provide specific information relating to alarms, such as:

— Trends for variables from which the alarm is derived;
— Statistics, such as how often, on average, the alarm has occurred;
— Relationships with other alarms or variables;
— Current or historical work orders or reports relating to the alarm.

Alarm response procedures

4.175. Paragraph 7.9 of SSR-2/2 (Rev. 1) [2] requires that procedures for operators to manage the response to alarms be established for all alarms in the control rooms.

4.176. Alarm response procedures should provide operators with the following information:

— The system or functional group to which the alarm belongs;
— The exact message associated with the alarm;
— Priorities for response to alarms;
— Automatic actions, and immediate and other operator actions;
— A list with the potential cause or causes of the alarm;
— References.

DEVELOPMENT OF PROCEDURES

4.177. This section provides recommendations on human factor aspects of procedure development and should be read in conjunction with the recommendations provided in IAEA Safety Standards Series No. NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants [11] and SSG-54 [10].

4.178. Important human tasks identified by safety analyses should be addressed in procedures.

4.179. The procedures that outline important human tasks, as identified by safety analyses, should be validated periodically to confirm:

— The availability and status of equipment necessary to successfully complete each procedure;

— The validity of any assumptions or claims made in safety analyses about tasks performed by humans that are related to safety.

4.180. Procedures should be validated to ensure that they can be executed as specified and that the results or outputs are as intended.

4.181. The development of procedures should also consider inputs from task analyses for the following purposes:

— To identify potential errors that need to be highlighted in the procedure;
— To describe the flow of information, actions and feedback necessary for the successful completion of a task;
— To identify links between tasks and personnel;
— To provide preliminary information on the timing of individual actions within the procedure;
— To facilitate the transition between procedures;
— To establish the format and content of technical warnings, prerequisites (initiating conditions) and requirements for termination of the procedure.

4.182. The expected outcome of an action (or suite of actions) identified in a procedure should be clear, understandable and verifiable.

4.183. In applying HFE to the development of plant procedures, the format and content associated with the category of procedure (e.g. emergency operating procedures, maintenance procedures and test procedures) should be taken into account.

4.184. Procedures for safety critical tasks, complex tasks and rarely performed tasks should be set out in a detailed and step by step manner.

4.185. Each procedure should provide guidance for safe alternative actions if the actions specified cannot be achieved or guidance for terminating the procedure safely.

DEVELOPMENT OF TRAINING PROGRAMMES

4.186. The task analysis should provide a basis (e.g. identification of knowledge, skills and abilities) for determining training requirements for the system being designed.

4.187. Operating personnel should be trained on the relationship between the display form and the plant states it is intended to represent, including failure modes and their effect and appearance on the display.

4.188. Operating personnel should be trained in navigation within and between displays, manipulation of on-screen features such as windows, and use of other functionalities within the HMI.

4.189. The training plan should be reviewed and modified periodically in accordance with the evolution of the design.

4.190. Training should be timely, and training associated with modifications to the plant should be completed prior to the modifications being put into effect.

4.191. The development of a training programme should follow the guidance provided in IAEA Safety Standards Series No. NS-G-2.8, Recruitment, Qualification and Training of Personnel for Nuclear Power Plants [12].

5. VERIFICATION AND VALIDATION IN RESPECT OF HUMAN FACTORS

GENERAL

5.1. Verification and validation of the HMI system in respect of human factors should comprehensively determine whether the HMI system conforms to specified HFE design requirements and whether it enables personnel to successfully and safely perform the intended functions in order to ensure safe operation of the plant.

5.2. Verification and validation should be implemented throughout the HFE design process, based on models and simulations that become increasingly realistic as the project progresses.

5.3. Verification and validation should provide objective evidence that designers have adhered correctly to design principles and requirements for usability in respect of human, technical and organizational aspects, and their interactions.

5.4. Verification activities typically include:

— Identification of HFE standards and guidelines;
— Verification of the HMI, including hardware (e.g. consoles, panels and analogue interfaces, including alarm displays) and software, and of associated documentation (e.g. procedures, instructions and alarm sheets);
— Review of design requirements, drawings and manuals;
— Verification of means to support tasks, including the provision of tools, job aids, personal protective equipment, task related equipment and training, the qualifications of operators, and the availability of accessible and usable procedures at the point of need.

5.5. Verification activities might involve interactions with system users.

5.6. Verification and validation activities are required to be undertaken by individuals or groups separate from those who originally performed the design work [1].

5.7. Validation should be performed, in particular, to evaluate:

— The ability of control room personnel to complete the required actions in operational states and accident conditions;
— The presentation and the organization of procedures to support task performance;
— The capability of the HMI to support operator tasks;
— The suitability of the layout of the workspace to support task and system performance;
— The resources for crisis management and coordination among the team members involved in the management of an accident, including external organizations.

5.8. Validation of the design of control rooms in respect of human factors should cover:

— The layout of the main and supplementary control rooms as it supports operator tasks;
— The effectiveness of the systems for monitoring, control and maintenance (inside and outside the control rooms);
— The monitoring and control systems in the control room linked to the entire plant for use in operational states and accident conditions.

5.9. Validation of the integrated system, comprising hardware, software, procedures and humans, should be performed before the design is finalized, so that enough time is available to make changes to the design before the plant becomes operational.

5.10. The inputs for verification and validation should originate from the HFE processes that have already been implemented, in particular:

— The concept of operations in all operational states and accident conditions;
— The technical and user requirements associated with the tasks, especially safety critical tasks;
— The functional and detailed specifications of the means of control and of the level of automation;
— Inputs from function analysis;
— Regulatory requirements;
— Inputs from the review of operating experience;
— Important human tasks;
— Data from safety analysis;
— Data from human reliability analysis;
— Data from the analysis of staffing, organization and qualifications;
— Data from previous HFE reviews and analyses;
— Input from simulation, where available (e.g. partial task simulation).

PLANNING FOR VERIFICATION AND VALIDATION

5.11. Verification and validation should be documented in a human factors verification and validation plan. The plan should lay out the level of independence and the resources, evaluation methods, and standards and regulations that apply.

5.12. Planning for verification and validation is an iterative activity that supports project changes as the design progresses, for example:

— As more interfaces become available;
— As procedures become more detailed;
— As operators are trained;
— As simulations become more realistic.

5.13. The verification and validation plan should specify:

— The scope of the evaluation;

— The necessary data collection and analysis;
— Measures of effectiveness;
— Evaluation and acceptance criteria;
— Participants involved in the evaluation;
— Training needs for the evaluation team, including for those participating as user representatives;
— The test environment;
— The schedule.

5.14. In addition, the verification and validation plan should also specify:

— The selection of scenarios;
— Materials[5] and tools to be used by the evaluation team.

5.15. The verification and validation plan should also describe the objective and the expected output that will demonstrate the compliance of the HMI design:

— With the project's HFE requirements (e.g. ergonomic requirements and project specific requirements);
— With the plant's operational acceptance criteria;
— With the regulatory requirements for operator response.

5.16. The verification and validation plan should also describe the following processes:

— The analysis and assessment of any HFE related issues;
— The tracking of HFE related issues;
— The approach for resolving design deficiencies.

5.17. The validation should be defined and conducted by a multidisciplinary validation team with different skills and expertise (e.g. specialists in the operation of the plant, instructors, experts in operations in the event of incidents and accidents, and HFE experts).

5.18. The participants conducting validation tests should be organized in accordance with the organizational structure for future operation of the plant.

[5] 'Materials' include audio recordings, video recordings, computer recordings and questionnaires.

5.19. The participants in validation tests should be representative of the plant personnel who will use the HMI (e.g. licensed operators rather than training or engineering personnel).

5.20. The validation team should be trained in data collection techniques.

TEST METHODS

5.21. Normally, verification and validation in respect of human factors should include all or a subset of the following;

- Static testing (e.g. to verify that the system meets the design specifications);
- Dynamic testing (e.g. testing of the system response in terms of time and accuracy);
- Scenario testing and partial task simulations or full scope simulations (e.g. testing of operator response in terms of time and accuracy);
- Observation;
- Independent reports (e.g. questionnaires and structured interviews);
- Checklists (e.g. within static or dynamic testing);
- Walkthroughs of tasks.

5.22. The test participants should be familiar with the relevant system before conducting the test.

5.23. The conformity and the limits of representativeness of the test beds, models and simulators used in the verification and validation tests should be justified.

PERFORMANCE MEASURES

5.24. Verification and validation in respect of human factors should apply relevant human performance measures for the actual working environment. Such measures could include:

- The complexity of the task to be performed;
- The workload (individual and team);
- The knowledge, skills and abilities required with respect to the design;
- Sequencing and response times;
- Requirements for situation awareness (individual and team);
- Requirements for using procedures;

— Requirements for detecting and responding to adverse conditions;
— Requirements for collaboration and communication between users and with other teams.

5.25. Possible qualitative and quantitative measures associated with human performance could include:

— Time;
— Accuracy;
— Communication frequency and content;
— Error detection and error recovery rates;
— Parameters relating to situation awareness (e.g. cue identification, comprehension and prediction);
— Use of group decision making methods;
— Gaze time and dwell time (e.g. from eye tracking);
— Fatigue;
— Probability of successful task performance.

VERIFICATION CRITERIA

5.26. The criteria applied for the verification should include HFE standards and guidelines used in the design. The selection of HFE standards and guidelines to be used in verification depends on the characteristics of the HMI components included in the scope of the evaluation.

5.27. Verification of HMI design should also be performed to identify whether task requirements that were identified in the HFE task analysis have been met (e.g. requirements relating to time constraints, sequence and precision).

VALIDATION TESTING

5.28. The test scenarios chosen to validate the design in respect of human factors should be realistic to the extent possible, including:

— Simulations and test beds should correspond to the design and physical layout of the plant.
— The tested scenarios should be representative of the operating conditions in all plant states and should include events (e.g. failures) and their initiating conditions.

— The operating tasks should be representative of those used in the plant (e.g. monitoring, detection, diagnosis, anticipation of changes in parameters, surveillance, control and manual recovery of automatic control systems).
— Participants should be trained and should occupy a position in the test scenario corresponding to their levels of qualification and responsibility.
— The procedures applied should match those that will be used in the relevant operating conditions.
— The range of human interactions expected during scenarios should be tested.

5.29. The plausibility of the tested situations and their representativeness should be justified.

DATA COLLECTION

5.30. The means of collecting data should be documented in the human factors verification and validation plan. The plan should specify the duration of tests or the number of trials for tests, the systems and subsystems to be tested, and the number of subjects from which data are to be collected.

5.31. Data collection should be undertaken in the course of the tests on mock-ups, partial task simulators in the field and full scope simulators, in order to evaluate, for example:

— The actions taken by the test participants (e.g. by means of manual collection of data by observers during each test);
— Communication between the test participants in the control room and communication between the control room and other teams involved in the operation of the plant and crisis management.

5.32. Data should be collected on deficiencies (i.e. the detected difficulties and mistakes made by the test participants) and also on the ease of use of tools anticipated by the design. Consequently, the validation tests should be used to identify the resources that provide support for operator actions for safety purposes and those for which improvements are necessary, for example:

— To facilitate the surveillance of the plant and to enhance situation awareness;
— To optimize the workload of personnel;
— To encourage cooperation and communication among personnel.

5.33. The means of collecting data in validation tests should be capable of making both objective measurements (e.g. measurements of the time taken to perform an action) and subjective measurements (e.g. measurements using a subjective questionnaire on the workload as perceived by the personnel).

5.34. The collected data should allow for in depth analysis of every tested situation, covering, for example:

— The chronology of the actions taken;
— The identification of tasks that were performed consistently well and without issues;
— The identification and analysis of unusual occurrences in the execution of the scenario (e.g. any difficulties encountered by personnel, hesitations about how to proceed and misunderstandings between the members of the control room team about the status of the systems or equipment).

5.35. The data collected during and after the test should be available for analysis.

DATA ANALYSIS

5.36. The analysis of the validation tests should involve in depth examination of the collected data. The analysis should cover both the mistakes made by the test participants as well as human activities that were performed successfully. Furthermore, in all the operating situations tested, the analysis should highlight:

— The systems that were used successfully by the test participants and that meet their needs;
— The systems that were difficult to use;
— The implied safety significance of the test results;
— Suggestions for improved design (made by both the analyst and users).

5.37. The analysis of the collected data should demonstrate the efficiency of the systems made available to the personnel and of the organizational provisions, and should demonstrate that, without an excessive workload, the test participants were able to:

— Comprehend the situation;
— Take the required actions, while taking the corresponding requirements into consideration;

— Cooperate with one another in the control room, and with the personnel with whom the control room staff have to interact (e.g. maintenance personnel, automatic control systems personnel and crisis management teams).

5.38. HFE related issues arising from the test campaign should be systematically documented and tracked.

5.39. The solutions applied to mitigate HFE related issues and the effectiveness of these solutions should be documented, evaluated and monitored.

5.40. The data collected in each test campaign and their analysis should be documented.

RESULTS

5.41. The results of each verification and validation test campaign should be documented.

5.42. A report on the verification and validation performed should be produced that summarizes the test plan, test findings, suggestions for improvements and conclusions.

5.43. Any gaps with the HFE standards and the safety objectives should be investigated, resolved and documented.

5.44. Any aspects that could not be addressed in the verification and validation tests, and that will have to be validated on the site after the plant enters operation, should be specified.

6. HUMAN FACTORS ENGINEERING DESIGN IMPLEMENTATION

6.1. The implementation of the design for human factors comprises the development, deployment and evaluation of the output from the human factors design process.

6.2. The design implementation should be performed as part of the formal construction and commissioning programmes, the licensing programme or plant modification processes.

6.3. The HFE design implementation should evaluate whether the as-built design conforms to the verified and validated design, and whether any unforeseen issues arise when the design is implemented in the actual plant and working environment.

6.4. The HFE design implementation should confirm that:

— The implementation of the design process matches its technical specification in terms of standards, functionality and safety performance;
— The implemented design has not generated any issues or conflicts (e.g. safety, operability or cultural aspects) relating to personnel, the management system, or structures, systems or components (e.g. inconsistencies with existing systems or interfaces).

6.5. The scope of the HFE design implementation should consider the impact of the design on the following elements:

— Organizational factors;
— Personnel factors;
— Job design;
— Safety analysis;
— Probabilistic safety assessment and human reliability analysis;
— The HMI;
— Equipment;
— Procedures;
— Training;
— Plant reference documentation;
— The working environment.

6.6. In the HFE design implementation stage, appropriate consideration should be given to the following aspects:

— An assessment that considers the consequences of the as-built design on actions that might be necessary to mitigate any undesirable consequences of HFE design implementation.
— Elements that need to be in place prior to commencing the implementation (e.g. the training of the implementation team on the use of simulators or

test beds that is necessary to ensure that they attain the desired level of task performance).
— A definition of criteria for successful implementation. This could link to the human performance monitoring system to ensure that the right aspects of human performance are being tested or measured.
— A method for capturing, assessing and resolving HFE related issues that are identified during the HFE design implementation stage.
— Where practicable, contingency strategies in the event that the HFE design implementation fails to meet its performance objectives.

6.7. The output of the HFE design implementation should be documented and evidence of the following items should be summarized:

— The outputs from the design project, including supporting provisions (e.g. the HMI, procedures and training), meet the relevant standards and performance and success criteria, as defined at the start of the project;
— Any negative effects on humans, technology and the organization are tolerable or suitably ameliorated;
— Any changes made to the as-built design are reflected in plant drawings and materials (e.g. training material, procedures, drawings, simulators, organizational structures and ancillary equipment);
— All HFE related issues identified prior to HFE design implementation have been adequately addressed;
— Any new HFE related issues have been captured and assessed, and a suitable plan for resolution has been established;
— Any remaining non-conformances have been assessed and deemed to be acceptable on safety grounds.

7. HUMAN PERFORMANCE MONITORING

7.1. Monitoring of human performance should be an active and ongoing process to evaluate the continuing effectiveness of the design in properly supporting personnel in carrying out their work tasks safely and effectively. Monitoring of human performance provides insights into:

— Whether the HMI design meets (and will continue to meet) the original safety, operability and performance assumptions;

— Whether the HMI design can be effectively used by operating personnel to conduct their tasks in the main control room, supplementary control room, local control stations and emergency response facilities;
— Whether changes made to the HMI design, procedures and training have any adverse effects on how operators carry out their work tasks;
— Whether human tasks can be accomplished in accordance with response time criteria and performance criteria;
— Whether the level of performance established at the stage of system validation is maintained over the lifetime of the plant;
— Whether the supporting provisions, such as supervision, training, staffing, procedures, personal protective equipment, tools and job aids, are appropriate and sufficient to support personnel in performing their tasks.

7.2. Human performance monitoring should consider the following:

— Individuals responsible for human performance monitoring, and the users of its outputs, should be adequately trained.
— Individuals responsible for human performance monitoring should be suitably qualified and experienced in the domains of human and organizational factors, systemic approaches and root cause analysis methods.
— The causes and significance of deficient human performance should be comprehensively understood and means for performance improvement should be identified.
— A culture of open and honest reporting should be established to ensure the effective use of issue reporting by system users.
— Individual and team performance is affected by human performance at all levels within the organization; therefore, effective human performance monitoring should capture data from all levels.
— Progress in responding to and resolving degraded human performance should be monitored to ensure that the response is within appropriate timescales.

7.3. Plant exercises and drills provide an important opportunity to gather information on human performance during a wide range of plant responses in all plant states. Where practicable, high levels of authenticity should be used to approximate the conditions faced during a real event.

7.4. In new build projects in which the operating organization is not the design authority, it should be ensured that assumptions made at the design stage about human performance are captured and validated in the commissioning and operation stages.

8. APPLICATION OF HUMAN FACTORS ENGINEERING IN DESIGN FOR COMPUTERIZED PROCEDURES

GENERAL

8.1. Computerized procedures might be used to support the operating personnel in monitoring and detection, situation assessment, response planning and response implementation tasks by transforming paper based procedures into digital form, so as to provide different levels of functionality, including varying levels of automation.

8.2. When computerized procedures are to be implemented at an existing plant, the HFE programme should consider how they will be introduced, in order to ensure proper functionality and consistency with the expectations and experience of operating personnel.

8.3. Computerized procedures should be included in the configuration management programme of the plant.

8.4. The design of computerized procedures should consider the practical feasibility of authoring, quality assurance, review, verification, validation, control and updating the procedures.

8.5. Computerized procedures systems are of three types:

— Type I systems represent an equivalent reproduction of paper based procedures and do not receive any processed or real time information.
— Type II systems augment procedures with dynamic embedded process data.
— Type III systems provide the capabilities of Type II systems and include embedded soft controls to manipulate plant equipment. Type III systems could include the capability for automated sequences of steps that automatically carry out the actions described in the procedure.

THE HUMAN–MACHINE INTERFACE FOR COMPUTERIZED PROCEDURES SYSTEMS

8.6. HFE should be applied in the design of computerized procedures for both new plants and existing plants.

8.7. The following HFE principles should be applied to computerized procedures:

— Display, to the extent reasonably achievable, only information relevant to the task to be performed;
— Continuously provide distinguishing information (e.g. title, revision number, date, plant name and unit) for each procedure;
— Maintain consistency of display and location of information, navigation aids, controls and other application menus for each display in the computerized procedures system;
— Arrange the computerized procedures system (including, for example, its structure, format, navigation menus and controls) to be adaptive to any device on which the system is going to be used.

8.8. An adequate number of displays should be used to provide the operator with all the information necessary to correctly carry out the procedure.

8.9. The HMI for computerized procedures should support easy navigation across the displays.

INTERACTION WITH THE COMPUTERIZED PROCEDURES SYSTEM

8.10. The recommendations on interaction capabilities set out in paras 8.11–8.20 are applicable to Type I, Type II and Type III computerized procedures, unless otherwise specified.

8.11. Warnings and cautions referred to in a procedure step should be displayed so that:

— They are presented when the step is on the display;
— They are read by the operator before the actions detailed in the step are carried out;
— Each warning or caution is presented in a way that is easily distinguished from other warnings or cautions.

8.12. Each set of related items should be presented in a list format that:

— Makes it easy for the operator to process the information;
— Clearly distinguishes each set of items from other sets of items;
— Includes a header specifying the content of the list.

8.13. The status of the steps of a procedure (e.g. whether the step is completed, in progress, checked and authorized where necessary, or failed) should be indicated. For Type I systems, the capability to manually track the status of steps should be provided. An indication of alternative action, where necessary, should also be included.

8.14. For Type II and Type III computerized procedures, the system should record and store the progress through the procedure. Multiple procedures within the computerized procedures system might need to be executed at the same time.

8.15. In such instances, human resources should be allocated appropriately and the execution of multiple procedures should be coordinated. For example, when more than one procedure is being carried out at the same time, the procedure and the status of steps in that procedure should be displayed on all devices.

8.16. The computerized procedures system should include features for navigation support that allow the operator to move within the procedure (between steps or to other parts of the same procedure) and from one procedure to another (e.g. through active links).

8.17. Notes, warnings and cautions should be accessible to the operator for all types of computerized procedure.

8.18. The data and logic rules that are used by the computerized procedures system should be available to the operator.

8.19. The computerized procedures system should provide operators with a means to record their annotations and comments regarding the execution of the procedure. These notes should be maintained and archived to be consulted later.

8.20. The computerized procedures system can suggest which procedure to use, but the responsibility for this decision should lie with the operators, who should take this decision on the basis of the plant status. This applies to Type II and Type III computerized procedures.

FUNCTIONAL CAPABILITIES OF THE COMPUTERIZED PROCEDURES SYSTEM

8.21. The computerized procedures system should notify the operator when the plant status necessitates entering a procedure, exiting a procedure or transitioning from one procedure to another.

8.22. Accurate information about the status of parameters and equipment should be automatically provided by the computerized procedures system.

8.23. Information and operator aids provided by the computerized procedures system should be context sensitive so that the operator does not receive inappropriate information.

8.24. The computerized procedures system might automatically process certain steps within a procedure. Results of the automatic processing of steps should be highlighted to the operator. The computerized procedures system should indicate those steps (e.g. time dependent steps and process dependent steps) for which continuous monitoring by the operator is necessary. The computerized procedures system should alert the operator when expected conditions in these steps are reached. In addition, the computerized procedures system should indicate whether the monitoring of parameters has stopped or is still ongoing.

8.25. The computerized procedures system, including soft controls to manipulate plant equipment (for Type III procedures), should provide the operator with the necessary information to support the effective use of these controls.

DEGRADATION AND FAILURES OF THE COMPUTERIZED PROCEDURES SYSTEM

8.26. Guidelines should be developed for switching to backup procedures (e.g. paper based procedures, backup hardware panels), as well as for switching back from backup procedures to computerized procedures, when appropriate.

8.27. Degraded conditions and failures necessitating a transition to backup procedures should be recognized and indicated by the computerized procedures system.

8.28. Paper based procedures used as backup procedures should be available and accessible to operators.

8.29. The structure and format of information in the computerized procedures should be compatible with the structure and format of information in backup procedures.

8.30. When a transition to a paper based backup procedure becomes necessary, the following information should be available:

— Procedures that were currently being carried out;
— Procedure steps already completed and those not completed, including the step in which the execution of the procedure was interrupted;
— Information about steps or conditions that were being monitored when the transition to backup procedures took place;
— The information necessary to continue the execution of the procedure where it was interrupted, avoiding repetition of steps already completed.

8.31. The transition guide to backup procedures should consider failure modes associated with the computerized procedures system and should specify required operator actions during failure of the computerized procedures system and after the computerized procedures system has been recovered. These actions should be described from the perspective of the operator.

8.32. The time necessary to undertake the transition to backup procedures should be validated as meeting the functional requirements for the computerized procedures.

8.33. Training on computerized procedures should include the specific steps necessary for the transition to paper based procedures.

AUTOMATIC SEQUENCING OF STEPS IN COMPUTERIZED PROCEDURES

8.34. The highest level of computerized procedures is automation (i.e. automated sequences of steps that carry out the actions described in the procedure). Automation of the sequences of procedure steps is only applicable to Type III procedures.

8.35. The execution of automated sequences in computerized procedures should be authorized and monitored by operators who are responsible for safe plant operation.

8.36. Operators should be able to choose whether to execute the steps of a computerized procedure manually or to activate automation.

8.37. Operators should be responsible for selecting which procedure is to be used.

8.38. Automated sequences of steps should be included in a single procedure (i.e. each sequence should begin and end within a single procedure).

8.39. Information on detailed and specific sequences of steps should be provided to operators by the computerized procedures system.

8.40. Information on the progress of automated sequences should also be provided to operators (i.e. information on completed, current and pending steps).

8.41. Information on failures of automation should be provided, along with the point in the sequence at which failure occurred.

8.42. Information on the necessary initial conditions to be satisfied before the execution of an automated sequence of steps can commence should be provided to operators by the computerized procedures system.

Hold points in automated sequences of steps

8.43. An automated sequence of steps could include a hold point, which is a predefined point in the procedure at which the progress of the procedure will halt, and the operator will be requested to acknowledge the status of the automated sequence and to authorize the procedure to continue.

8.44. Hold points should be included in the automated sequences to:

— Assist the operator in recognizing the progress of the automation and in making any relevant and necessary decisions or adjustments for the procedure to continue;
— Maintain the operator's awareness of the status of plant equipment involved in the sequence of steps being carried out;
— Enable the operator to authorize the procedure to continue.

8.45. The computerized procedures system should allow the operator to include additional temporary hold points before starting an automated sequence of steps.

8.46. The computerized procedures system should not allow the operator to remove predefined hold points.

8.47. Hold points defined in a procedure should leave the procedure in a stable condition in which the operator is able to correctly evaluate the status of the procedure and to make the necessary decisions for the procedure to continue.

Interruption of automated sequences of steps

8.48. Upon interruption of automated sequences of steps, the computerized procedures system should allow the operator either to transition safely from automatic to manual execution or to resume automatic execution.

8.49. Information on the interruption, such as why the sequence was interrupted, which steps have been completed and which steps are still to be executed, should be provided by the computerized procedures system.

8.50. The computerized procedures system should be able to automatically interrupt an automated sequence in the event that a necessary condition for the step to be completed is not met, or the safe completion of the current step cannot be guaranteed for any other reason.

8.51. The computerized procedures system should alert the operator to any interruption of an automated sequence.

9. INTEGRATION OF HUMAN FACTORS ENGINEERING INTO SAFETY PROCESSES

DEVELOPMENT AND REVIEW OF THE SAFETY ANALYSIS REPORT

9.1. The content of the chapter in the safety analysis report on HFE should describe the HFE programme and its application to the specific plant design.

9.2. HFE considerations presented in the safety analysis report should cover, at a minimum:

— HFE programme management, including the authority and oversight for HFE in the design process;

— The human factors analysis methods applied;
— Assumptions for the choice of HMI design, with account taken of HFE;
— Human factors verification and validation, including the identification and resolution of HFE related issues during the design project and assumptions made during analysis;
— A description of how the HMI design has been implemented in the plant as a whole;
— A description of the strategy for human performance monitoring for safety critical tasks.

9.3. A review should be conducted to verify that acceptable HFE practices and guidelines were incorporated into the design and the safety analysis report.

9.4. Whenever manual actions are credited in the safety analysis as backups to automatic actions, consideration should be given to including HFE analysis in the design analysis to contribute to diversity.

9.5. Modifications of the plant in respect of human factors should be documented in the safety analysis report.

9.6. Recommendations on the format and content of the safety analysis report are provided in IAEA Safety Standards Series No. SSG-61, Format and Content of the Safety Analysis Report for Nuclear Power Plants [13].

PLANT MODIFICATIONS

9.7. Paragraph 4.40 of SSR-2/2 (Rev. 1) [2] states: "Consequences of the modification for human tasks and performance shall be systematically analysed. For all plant modifications, human and organizational factors shall be adequately considered."

9.8. A review of HFE aspects should be conducted to identify the potential impact on risk whenever a modification of human tasks results from modifications to the plant. This applies for both small scale and large scale modifications.

9.9. A review of HFE aspects should be conducted whenever changes (e.g. in sequencing, timing and workload) are made to procedures for which credit is taken in the safety analysis.

9.10. A graded approach should be applied to the HFE programme for plant modifications.

9.11. Any modification involving HFE solutions should be incorporated into plant controls (e.g. documentation, procedures, layout, administrative controls and training) before the modification is implemented.

9.12. Recommendations on controlling activities relating to modifications to nuclear power plants are provided in IAEA Safety Standards Series No. NS-G-2.3, Modifications to Nuclear Power Plants [14].

PERIODIC SAFETY REVIEW

9.13. This section provides recommendations on HFE activities that can support the recommendations provided in IAEA Safety Standards Series No. SSG-25, Periodic Safety Review for Nuclear Power Plants [15].

9.14. The periodic safety review should confirm whether assumptions made about the following continue to be valid:

— The most resource intensive conditions feasible for each operational mode or plant state;
— The feasibility of the division and coordination of work in the most resource intensive conditions, as assessed by function allocation, task analyses and workload analyses.

9.15. The periodic safety review should consider whether the staffing, organization, system design, training, procedures, tools, equipment and other resources necessary for successful human performance are suitable and sufficient for the most resource intensive conditions.

9.16. The periodic safety review should consider whether HFE verification and validation activities, as described in Section 5, used to confirm assumptions and claims in respect of human tasks identified in safety analyses, continue to be valid.

9.17. The periodic safety review should consider whether the assumptions made regarding staff competencies are aligned with human limitations and capabilities, task requirements and regulatory requirements.

9.18. The periodic safety review should be used to identify reasonably practicable improvements in managing human and organizational factors to ensure that successful human performance is achieved, including through the HFE programme.

10. APPLICATION OF HUMAN FACTORS ENGINEERING IN PRODUCT SELECTION AND PROCUREMENT

10.1. This section provides recommendations on HFE aspects for the selection, procurement, integration and use of several products, such as personal protective equipment (e.g. for maintenance, inspections, accident monitoring and operation of equipment for severe accident mitigation), commercial off the shelf products and mobile devices (e.g. hand-held, portable and wearable devices).

PERSONAL PROTECTIVE EQUIPMENT

10.2. Personal protective equipment and its characteristics should be selected to be compatible with the users' body sizes, the tasks to be performed while wearing it, and the range of environments in which the users are expected to work. HFE design criteria that relate to the use of personal protective equipment should be applied to the anticipated use of the equipment and the tools and job aids that are permitted to be used while wearing it.

10.3. Personal protective equipment should not significantly affect the reliability of task performance.

10.4. HFE analysis should be conducted to determine whether the task can be carried out while using personal protective equipment, which might affect users' vision, hearing, dexterity, mobility or ability to work in extreme temperatures.

10.5. Personal protective equipment should be verified and validated in accordance with its intended use under various plant conditions (e.g. by means of drills and emergency exercises). This verification and validation should consider the full range of body sizes of the users.

COMMERCIAL OFF THE SHELF PRODUCTS

10.6. Where commercial off the shelf products are integrated into an existing system, human factors should be considered in selecting those products that are consistent with the plant's design, operation and maintenance strategy.

10.7. Where a commercial off the shelf product or various commercial off the shelf products are integrated into a new or existing system, consideration should be given to selecting those products that would ensure HMI characteristics consistent:

— Within each system;
— Between similar systems that are already used by operators;
— With existing characteristics of the HMI at the plant.

10.8. Where a commercial off the shelf product is to be incorporated into an existing system, the impact on human performance should be assessed.

10.9. HFE should be applied to ensure that the installation of a commercial off the shelf product does not result in undesirable changes in the working environment or in the way that tasks are performed.

10.10. HFE should be applied to determine whether the installation of a commercial off the shelf product requires additional training, modified or new procedures, maintenance or testing, or changes in skills and qualification requirements.

MOBILE DEVICES

10.11. The scope of the review of mobile devices should include hand-held, portable and wearable devices.

10.12. The selection of mobile devices should be based on analyses that reveal whether the mobile device is appropriate for the task and the length of time that users need to be able to hold, interact with, transport or wear the device. The mobile device should also be appropriate for the task if users are wearing personal protective equipment.

10.13. Mobile devices and their characteristics should be selected to be compatible with the users' body sizes, the environmental conditions and HFE

design criteria (e.g. for lighting, grip, size, weight and characteristics of human information processing).

10.14. Mobile devices should not interfere with the accomplishment of other tasks when they are not in use.

10.15. Where appropriate, information regarding requirements for mobile devices in extreme environments (e.g. the use of rugged devices) should be known to users.

10.16. The storage of mobile devices should be considered in HFE analyses.

10.17. Requirements for the synchronization or calibration of mobile devices should be considered.

10.18. For mobile computing devices, error management is of high importance for safety because of the potential constraints on using the device. HFE should determine the need for:

— Error correction functions (e.g. an easy means for correcting erroneous entries and for correcting individual errors without the need for correctly entered commands or data to be re-entered);
— Features for early detection and correction of errors by users and software, after keying in, but before entry into the system;
— Error checking in a manner that does not disrupt the user (e.g. at the end of data fields rather than character by character);
— User control of the process when equipment is controlled from a mobile device (e.g. capability to stop the process at any point in the sequence as a result of an indicated error).

10.19. The potential for interference from high intensity radiation fields should be considered as such radiation fields are likely to pose design constraints.

REFERENCES

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

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

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Operating Experience Feedback for Nuclear Installations, IAEA Safety Standards Series No. SSG-50, IAEA, Vienna (2018).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004). (A revision of this Safety Guide is in preparation.)

[9] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-54, IAEA, Vienna (2019).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000). (A revision of this Safety Guide is in preparation.)

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Recruitment, Qualification and Training of Personnel for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.8, IAEA, Vienna (2002). (A revision of this Safety Guide is in preparation.)

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Format and Content of the Safety Analysis Report for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-61, IAEA, Vienna (in preparation).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Modifications to Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.3, IAEA, Vienna (2001). (A revision of this Safety Guide is in preparation.)
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-25, IAEA, Vienna (2013).

Annex

BIBLIOGRAPHY OF INTERNATIONAL INSTRUMENTATION AND CONTROL, AND HUMAN FACTORS ENGINEERING STANDARDS

A–1. Requirement 9 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [A–1] states: "**Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.**"

A–2. This Safety Guide provides high level recommendations that are widely accepted among IAEA Member States. Beyond the guidance provided by the IAEA, a large body of national and international standards exists that give more detailed recommendations about design methodologies and system characteristics that support compliance with SSR-2/1 (Rev. 1) [A–1]. It is expected that designers, operating organizations and regulatory bodies will take advantage of the information in these standards.

A–3. Two standards development organizations are responsible for most of the internationally used standards for I&C systems in nuclear power plants: the International Electrotechnical Commission (IEC; Subcommittee 45) and the Institute of Electrical and Electronics Engineers (IEEE; Nuclear Power Engineering Committee). Each organization has developed a large number of standards. Both organizations produce standards that respond to the common principles underlying the requirements of SSR-2/1 (Rev. 1) [A–1] and the recommendations of this Safety Guide. Consequently, either set of standards can be used to further interpret the recommendations of this Safety Guide.

A–4. This Annex is intended to help readers understand the relationship between this Safety Guide and the IEC and IEEE standards. Table A–1 lists the IEC and IEEE standards that have a strong relationship with the recommendations of this Safety Guide. Table A–1 is not a complete list of either set of standards, but it identifies the entry points into the sets of IEC and IEEE standards.

A–5. Table A–2 shows how these entry standards relate to the major topical areas of this Safety Guide.

A–6. A concerted effort was made to avoid conflicts between the recommendations of this Safety Guide and the standards of the IEC and IEEE. Members of both the IEC and the IEEE standards committees participated in the

development of this Safety Guide, and both standards organizations reviewed drafts to help identify and eliminate conflicts.

A–7. Nevertheless, users need to recognize and take account of the fact that there are important differences between the IEC and the IEEE standards. IEC standards take the IAEA Safety Requirements publications and Safety Guides as fundamental inputs for their development. As a result, the IEC standards deal with items important to safety and take the guidance on I&C systems provided by the IAEA as the source of general recommendations.

A–8. IEEE standards focus largely on items important to safety, and therefore the IEEE guidance directly applies to a smaller set of functions, systems and equipment than this Safety Guide does. Nevertheless, the guidance of the IEEE can be applied to safety related items (items important to safety that are not safety systems) using a graded approach.

A–9. Other guidance documents (e.g. NUREG series publications) include reports or brochures on regulatory decisions, results of research, results of incident investigations, and other technical and administrative information. Table A–2 shows how these other guidance documents relate to the major topical areas of this Safety Guide.

TABLE A–1. INTERNATIONAL STANDARDS WITH A STRONG RELATIONSHIP TO THIS SAFETY GUIDE

International standard	Title
IEC 60960:1988 [A–2]	Functional Design Criteria for a Safety Parameter Display System for Nuclear Power Stations
IEC 60964:2018 RLV [A–3]	Nuclear Power Plants — Control Rooms — Design
IEC 60965:2016 [A–4]	Nuclear Power Plants — Control Rooms — Supplementary Control Room for Reactor Shutdown without Access to the Main Control Room
IEC 61227:2008 [A–5]	Nuclear Power Plants — Control Rooms — Operator Controls
IEC 61771:1995 [A–6]	Nuclear Power Plants — Main Control-room — Verification and Validation of Design
IEC 61772:2009 [A–7]	Nuclear Power Plants — Control Rooms — Application of Visual Display Units (VDUs)
IEC 61839:2000 [A–8]	Nuclear Power Plants — Design of Control Rooms — Functional Analysis and Assignment
IEC 62241:2004 [A–9]	Nuclear Power Plants — Main Control Room — Alarm Functions and Presentation
IEEE 845-1999 [A–10]	IEEE Guide for the Evaluation of Human-system Performance in Nuclear Power Generating Stations
IEEE 1023-2004 [A–11]	IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities
IEEE 1082-2017 [A–12]	IEEE Guide for Incorporating Human Reliability Analysis into Probabilistic Risk Assessments for Nuclear Power Generating Stations and Other Nuclear Facilities
IEEE 1289-1998 [A–13]	IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-based Monitoring and Control Displays for Nuclear Power Generating Stations
IEEE 1707-2015 [A–14]	IEEE Recommended Practice for the Investigation of Events at Nuclear Facilities
IEEE 1786-2011 [A–15]	IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities

Note: IEC: International Electrotechnical Commission; IEEE: Institute of Electrical and Electronics Engineers.

TABLE A–2. RELATIONSHIP BETWEEN INTERNATIONAL STANDARDS, RELEVANT GUIDES AND THE TOPICAL AREAS OF THIS SAFETY GUIDE

Section in this Safety Guide	Internationally used I&C standards
1. Introduction	
2. Human factors engineering programme management	IEC 61513:2011 [A–16], IEEE 1023-2004 [A–11], IEEE 1074-2006 [A–17], ISO/IEC/IEEE 15288:2015 [A–18], NUREG-0711 (Rev. 3) [A–19], INL/CON-12-25117 [A–20], ISO 11064-1–7 [A–21 to A–27]
3. Analysis	IEC 61839:2000 [A–8], IEEE 845-1999 [A–10], IEEE 1082-2017 [A–12], NUREG-0711 (Rev. 3) [A–19], IEEE 1707-2015 [A–14], NUREG/CR-6400 [A–28]
4. Design:	
— Control rooms	IEC 60964:2018 RLV [A–3], IEC 61227:2008 [A–5], IEC 61771:1995 [A–6], IEC 61772:2009 [A–7], IEC 61839:2000 [A–8], IEC 62241:2004 [A–9], IEEE 576-2000 [A–29], IEEE 1289-1998 [A–13], NUREG-0700 (Rev. 2) [A–30], EPRI — Human Factors Guidance for Control Room Design and Digital Human–system Interface Design and Modification (2015) [A–31]
— Supplementary control rooms	IEC 60965:2016 [A–4], NUREG-0700 (Rev. 2) [A–30]
— Safety parameter display systems	IEC 60960:1988 [A–2], IEEE 497-2016 [A–32], NUREG-0700 (Rev. 2) [A–30], NUREG-0696 [A–33]
— General principles relating to human factors engineering for instrumentation and control systems	IEEE 1023-2004 [A–11], IEEE 1082-2017 [A–12], IEEE 1289-1998 [A–13]
5. Verification and validation in respect of human factors	NUREG-0711 (Rev. 3) [A–19]
6. Human factors engineering design implementation	IEC 61839:2000 [A–8], IEEE 845-1999 [A–10], IEEE 1082-2017 [A–12], NUREG-0711 (Rev. 3) [A–19]
7. Human performance monitoring	IEEE 845-1999 [A–10], NUREG-0711 (Rev. 3) [A–19]

TABLE A–2. RELATIONSHIP BETWEEN INTERNATIONAL STANDARDS, RELEVANT GUIDES AND THE TOPICAL AREAS OF THIS SAFETY GUIDE (cont.)

Section in this Safety Guide	Internationally used I&C standards
8. Application of human factors engineering in design for computerized procedures	IEC 62646:2016 [A–34], IEEE 1786-2011 [A–15]
9. Integration of human factors engineering into safety processes:	IEC 61772:2009 [A–7], IEC 62241:2004 [A–9], IEEE 1289-1998 [A–13], NUREG-0711 (Rev. 3) [A–19]
— General principles relating to human factors engineering for instrumentation and control systems	IEC 61513:2011 [A–16], IEEE 1023-2004 [A–11], IEEE 1082-2017 [A–12], IEEE 1289-1998 [A–13]

REFERENCES TO THE ANNEX

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

[A–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Design Criteria for a Safety Parameter Display System for Nuclear Power Stations, IEC 60960:1988, IEC, Geneva (1988).

[A–3] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Design, IEC 60964:2018 RLV, IEC, Geneva (2018).

[A–4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Supplementary Control Room for Reactor Shutdown without Access to the Main Control Room, IEC 60965:2016, IEC, Geneva (2016).

[A–5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Operator Controls, IEC 61227:2008, IEC, Geneva (2008).

[A–6] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Main Control-room — Verification and Validation of Design, IEC 61771:1995, IEC, Geneva (1995).

[A–7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Application of Visual Display Units (VDUs), IEC 61772:2009, IEC, Geneva (2009).

[A–8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Design of Control Rooms — Functional Analysis and Assignment, IEC 61839:2000, IEC, Geneva (2000).

[A–9] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Main Control Room — Alarm Functions and Presentation, IEC 62241:2004, IEC, Geneva (2004).

[A–10] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Guide for the Evaluation of Human-system Performance in Nuclear Power Generating Stations, IEEE 845-1999, IEEE, Piscataway, NJ (1999).

[A–11] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE 1023-2004, IEEE, Piscataway, NJ (2004).

[A–12] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Guide for Incorporating Human Reliability Analysis into Probabilistic Risk Assessments for Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE 1082-2017, IEEE, Piscataway, NJ (2017).

[A–13] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-based Monitoring and Control Displays for Nuclear Power Generating Stations, IEEE 1289-1998, IEEE, Piscataway, NJ (1998).

[A–14] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for the Investigation of Events at Nuclear Facilities, IEEE 1707-2015, IEEE, Piscataway, NJ (2015).

[A–15] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE 1786-2011, IEEE, Piscataway, NJ (2011).

[A–16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems, IEC 61513:2011, IEC, Geneva (2011).

[A–17] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Developing a Software Project Life Cycle Process, IEEE 1074-2006, IEEE, Piscataway, NJ (2006).

[A–18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Systems and Software Engineering — System Life Cycle Processes, ISO/IEC/IEEE 15288:2015, ISO, Geneva (2015).

[A–19] NUCLEAR REGULATORY COMMISSION, Human Factors Engineering Program Review Model, Rep. NUREG-0711 (Rev. 3), NRC, Washington, DC (2012).

[A–20] HUGO, J., Towards a Unified HFE Process for the Nuclear Industry, Rep. INL/CON-12-25117, Idaho National Laboratory, Idaho Falls, ID (2012).

[A–21] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 1: Principles for the Design of Control Centres, ISO 11064-1:2000, ISO, Geneva (2000).
[A–22] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 2: Principles for the Arrangement of Control Suites, ISO 11064-2:2000, ISO, Geneva (2000).
[A–23] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 3: Control Room Layout, ISO 11064-3:1999, ISO, Geneva (1999).
[A–24] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 4: Layout and Dimensions of Workstations, ISO 11064-4:2013, ISO, Geneva (2013).
[A–25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 5: Displays and Controls, ISO 11064-5:2008, ISO, Geneva (2008).
[A–26] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 6: Environmental Requirements for Control Centres, ISO 11064-6:2005, ISO, Geneva (2005).
[A–27] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 7: Principles for the Evaluation of Control Centres, ISO 11064-7:2006, ISO, Geneva (2006).
[A–28] NUCLEAR REGULATORY COMMISSION, Human Factors Engineering (HFE) Insights for Advanced Reactors Based Upon Operating Experience, Rep. NUREG/CR-6400, NRC, Washington, DC (1997).
[A–29] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for Installation, Termination, and Testing of Insulated Power Cable as Used in Industrial and Commercial Applications, IEEE 576-2000, IEEE, Piscataway, NJ (2000).
[A–30] NUCLEAR REGULATORY COMMISSION, Human-system Interface Design Review Guidelines, Rep. NUREG-0700 (Rev. 2), NRC, Washington, DC (2002).
[A–31] ELECTRIC POWER RESEARCH INSTITUTE, Human Factors Guidance for Control Room Design and Digital Human–system Interface Design and Modification, EPRI, Palo Alto, CA (2015).
[A–32] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, IEEE 497-2016, IEEE, Piscataway, NJ (2016).
[A–33] NUCLEAR REGULATORY COMMISSION, Functional Criteria for Emergency Response Facilities, Rep. NUREG-0696, NRC, Washington, DC (1981).
[A–34] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Computer-based Procedures, IEC 62646:2016, IEC, Geneva (2016).

DEFINITIONS

The following definitions are specific to this publication and are either not provided in, or are different from, those provided in the IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2018 Edition).

The symbol '' denotes a definition that differs from that provided in the IAEA Safety Glossary.*

computerized procedures system. A system that presents plant procedures in a computer based rather than a paper based format.

concept of operations.* A concept of operations describes the proposed design in terms of how it will be operated to perform its functions, which includes the various roles of personnel and how they will be organized, managed and supported. The concept of operations describes how the plant is operated ('operating philosophy') and includes aspects such as the number and composition of operating personnel and how they operate the plant under normal and abnormal conditions.

error management. Based on theories of perception, cognitive bias and anthropometry, this identifies the likelihood of errors made by humans in the system and technology interface. Human factors engineering predicts errors and then designs to prevent the errors or their consequences from impacting the safe operation of the plant.

human–machine interface. The human–machine interface is the part of a system through which personnel interact with the system to perform their functions and tasks. The human–machine interface constitutes the interface between personnel and plant systems, including procedures, communication systems displays, alarms and controls.

human motor control. Human motor control is the physiological capability of a human's muscular system to control movement, including strength and fine movements.

important human task. A human task that can have an adverse or positive effect on safety, as determined by safety analysis.

situation awareness. The dynamic process of perception and comprehension of the plant's actual condition in order to support the ability of individuals and teams to predict the future conditions of systems. It is a way of forming a mental model of the situation and future planned actions. The degree of situation awareness corresponds to the difference between the understanding of plant conditions and the actual conditions at any given time. One of the objectives of human factors engineering is to support the development of situation awareness in operating personnel.

validation.* Confirmation by examination and by means of objective evidence that the human–machine interface system as a whole, including the user, can successfully perform its intended functions and meet its goals and objectives in the range of environments in which it is anticipated to have to operate.

verification.* Confirmation by examination and by means of objective evidence that the human–machine interface system as a whole meets the design specifications and requirements, and provides the support necessary to accomplish tasks, as intended.

CONTRIBUTORS TO DRAFTING AND REVIEW

Duchac, A.	International Atomic Energy Agency
Gertman, D.	Idaho National Laboratory, United States of America
Hata, T.	Nuclear Regulation Authority, Japan
Humbel, C.	Swiss Federal Nuclear Safety Inspectorate, Switzerland
Illobre, F.	Tecnatom, Spain
Ito, K.	MHI Nuclear Systems and Solution Engineering, Japan
Johansson, Y.	Swedish Radiation Safety Authority, Sweden
Laarni, J.	Technical Research Centre, Finland
Ngo, C.	Candesco, Canada
Obenius Mowitz, A.	Swedish Radiation Safety Authority, Sweden
O'Hara, J.	Brookhaven National Laboratory, United States of America
Rycraft, H.	International Atomic Energy Agency
Screeton, R.	Office for Nuclear Regulation, United Kingdom
Selmer, S.	Swedish Radiation Safety Authority, Sweden
Tasset, D.	Institute for Radiological Protection and Nuclear Safety, France
Yllera, J.	International Atomic Energy Agency

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

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

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

NORTH AMERICA

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

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

REST OF WORLD

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

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

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

Individual orders:
www.eurospanbookstore.com/iaea

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

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

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

FUNDAMENTAL SAFETY PRINCIPLES
IAEA Safety Standards Series No. SF-1
STI/PUB/1273 (21 pp.; 2006)
ISBN 92–0–110706–4 Price: €25.00

GOVERNMENTAL, LEGAL AND REGULATORY FRAMEWORK FOR SAFETY
IAEA Safety Standards Series No. GSR Part 1 (Rev. 1)
STI/PUB/1713 (42 pp.; 2016)
ISBN 978–92–0–108815–4 Price: €48.00

LEADERSHIP AND MANAGEMENT FOR SAFETY
IAEA Safety Standards Series No. GSR Part 2
STI/PUB/1750 (26 pp.; 2016)
ISBN 978–92–0–104516–4 Price: €30.00

RADIATION PROTECTION AND SAFETY OF RADIATION SOURCES: INTERNATIONAL BASIC SAFETY STANDARDS
IAEA Safety Standards Series No. GSR Part 3
STI/PUB/1578 (436 pp.; 2014)
ISBN 978–92–0–135310–8 Price: €68.00

SAFETY ASSESSMENT FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GSR Part 4 (Rev. 1)
STI/PUB/1714 (38 pp.; 2016)
ISBN 978–92–0–109115–4 Price: €49.00

PREDISPOSAL MANAGEMENT OF RADIOACTIVE WASTE
IAEA Safety Standards Series No. GSR Part 5
STI/PUB/1368 (38 pp.; 2009)
ISBN 978–92–0–111508–9 Price: €45.00

DECOMMISSIONING OF FACILITIES
IAEA Safety Standards Series No. GSR Part 6
STI/PUB/1652 (23 pp.; 2014)
ISBN 978–92–0–102614–9 Price: €25.00

PREPAREDNESS AND RESPONSE FOR A NUCLEAR OR RADIOLOGICAL EMERGENCY
IAEA Safety Standards Series No. GSR Part 7
STI/PUB/1708 (102 pp.; 2015)
ISBN 978–92–0–105715–0 Price: €45.00

REGULATIONS FOR THE SAFE TRANSPORT OF RADIOACTIVE MATERIAL, 2018 EDITION
IAEA Safety Standards Series No. SSR-6 (Rev. 1)
STI/PUB/1798 (165 pp.; 2018)
ISBN 978–92–0–107917–6 Price: €49.00

Safety through international standards

"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."

Yukiya Amano
Director General

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–100419–2
ISSN 1020–525X