Date: 17 July 2017

IAEA SAFETY STANDARDS

for protecting people and the environment

Draft I

Step 10

Second internal review of the draft publication

Note:

Resolution to Member States comments can be seen in Draft H, step 9. Several Member States comments recommended re-organization of several sections and deleting several paras. With this regard, this revision I, step 10 proposes several modifications to the original document structure as follows:

– Severe accidents moved from section 8 under the Emergency response facility in Section 4;and
– Computerized procedures made a standalone Section 8;
– HFE integration in safety processes and HFE in product selection and procurement made stand-alone sections.

Comments resolution to specific paras remains the same as in Draft G, Step 9.

Human Factors Engineering in the Design of Nuclear Power Plants

DS-492

DRAFT SAFETY GUIDE

New Safety Guide

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide provides recommendations on the human factors engineering (HFE) to meet the requirements established in IAEA Safety Standards Series No. 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 publication takes into account developments, experience and practices in integrating human factors engineering into the design of nuclear facilities throughout the plant lifecycle. It references and takes into account other IAEA Safety Standards that are relevant and relating to HFE design. Most notable among these are the Safety Requirements GSR Part 2 [4], Leadership and Management for Safety, and its supporting Safety Guides GS-G-3.1 [5], Application of the Management System for Facilities and Activities, and GS-G-3.5 [6], The Management System for Nuclear Installations.

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

— Considerations specific to HFE, including the human machine interface for achieving compliance with the requirements established in Ref. [1];

— Integrating HFE into the design of nuclear facilities throughout the plant lifecycle for achieving compliance with the requirements established in Ref. [4];

— The HFE process to be considered in achieving human machine interface design across plant states;

— The HFE performance monitoring, evaluation and integration into safety processes, applications and product selection.

1.4. This Safety Guide provides a consideration of HFE aspects for several important processes linked to design, such as:

— Development and review of the safety analysis report;

— Plant modifications and modernizations for achieving compliance with the requirements established in Ref. [2];

— Periodic safety review.

1.5. This Safety Guide provides a consideration of relevant HFE aspects for design and use of computerized procedures.

1.6. This Safety Guide provides a consideration of relevant HFE aspects for selections, procurement, integration and use of several products in existing plant systems, such as:

— Personal protective equipment (e.g. used during maintenance activities, inspections, accident monitoring and operation of severe accident mitigation equipment);

— Commercial off the shelf products;

— Mobile devices (e.g. hand held, portable, and wearable).

1.7. Additional guidance on HFE design and development of human machine interface (HMI) is available from Member States and from other organizations that develop industrial standards. Such standards give much greater detail than is appropriate for IAEA safety standards. It is expected that this Safety Guide will be used in conjunction with detailed industry standards as suggested in Annex I.

OBJECTIVES

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

1.9. The Safety Guide identifies the input information needed to design and validate the human machine interface and the basis for human, physical and cognitive processes.

SCOPE

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

1.11. This Safety Guide is meant to be applied using the approach defined in Ref. [4].

1.12. This Safety Guide applies to implementation of the HFE aspects of the HMI design operation and maintenance for new plant designs as well as for modifications of existing plants.

1.13. This Safety Guide is intended for use by organizations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning for 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 intentional unauthorized acts.

STRUCTURE

1.15. Section 2 provides guidance for the management of a HFE programme. Section 3 provides recommendations for HFE analyses of operating experience, functional requirements and allocation, tasks, staffing, organization, qualification and important human tasks. Section 4 provides recommendations for HFE design. Section 5 provides guidance on verification and validation of

human factors in the design process. Section 6 provides recommendations on implementation of the HMI design. Section 7 provides recommendations on monitoring human performance aspect of systems performance during the plant operation. Section 8 provides recommendations on HFE design for computerized procedures, alarm filtering and management. Section 9 addresses topics related to HFE integration in safety processes. Section 10 addresses topics related to HFE in product selection specification for subcontracted procurements.

1.16. Annex I provides a list of international I&C and HFE standards, which are not Safety Standards but have a strong relationship with the major topical areas of this Safety Guide.

2. HFE PROGRAMME MANAGEMENT

GENERAL

2.1. GSR Part 2 [4] establishes requirements for the management systems for all types of facilities and activities.

2.2. Requirement 6 of GSR Part 2 [4] states that:

> "The management system shall integrate its elements, including safety, health, environmental, security, quality, human-and-organizational-factors, societal and economic elements, so that safety is not compromised."

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

"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 ensure successful integration of human characteristics and capabilities with nuclear power plant design, test, operation and maintenance.

2.5. HFE in design should be a planned and documented process as an integral part of any nuclear power plant project.

2.6. A HFE programme should be developed and documented.

2.7. The HFE programme should understand a nuclear facility as a system comprising the elements human, technology and organization by considering the dynamic interactions within and among all relevant factors:

— Human factors (e.g. knowledge and expertise, cognition, performance expectations, motivation, stress, strength and anthropometry);

— 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, the roles and responsibilities of managers and plant personnel).

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

2.9. The HFE programme should apply a questioning and learning attitude to accepted design methods and solutions, taking newly developed information, analysis methods, knowledge and features of new technology into account.

2.10. The HFE programme should follow the approach defined in Ref. [4] in order to identify the appropriate level of rigor, resources, and detail to be applied.

2.11. The HFE programme should outline the HFE processes as well as inputs and outputs for these processes. The HFE processes include analyses, design of human machine interface, evaluations, such as verification and validation, and monitoring of human performance.

2.12. The HFE programme should identify the integration of HFE with other plant design or modification activities.

2.13. The HFE programme should identify the coordination required between personnel responsible for the HFE programme, project and design authorities, and different disciplines in order to perform HFE activities.

2.14. The process for communicating outputs of analyses to the responsible engineering disciplines and ensuring that the outputs have been addressed should be documented.

2.15. The HFE programme should identify the responsible organization and competence requirements (e.g. qualification, skills, knowledge, training) for personnel performing human factors engineering.

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

2.17. The HFE programme should specify that HFE has representation in the design team, as opposed to being remote to the design team.

2.18. For the new plant design, the utility should assure itself that the intended plant design has followed appropriate HFE standards and elements of this Safety Guide.

THE HFE PROCESS MODEL

2.19. The HFE process can be grouped under the following:

— Programme management;

— Analysis;

— Design;

— Verification and validation;

— Design implementation;

— Human performance monitoring.

HFE ACTIVITIES WITHIN ENGINEERING PHASES

2.20. Interactions of HFE activities should be integrated into the basic phases of an engineering process as illustrated by the example provided in Fig.1.

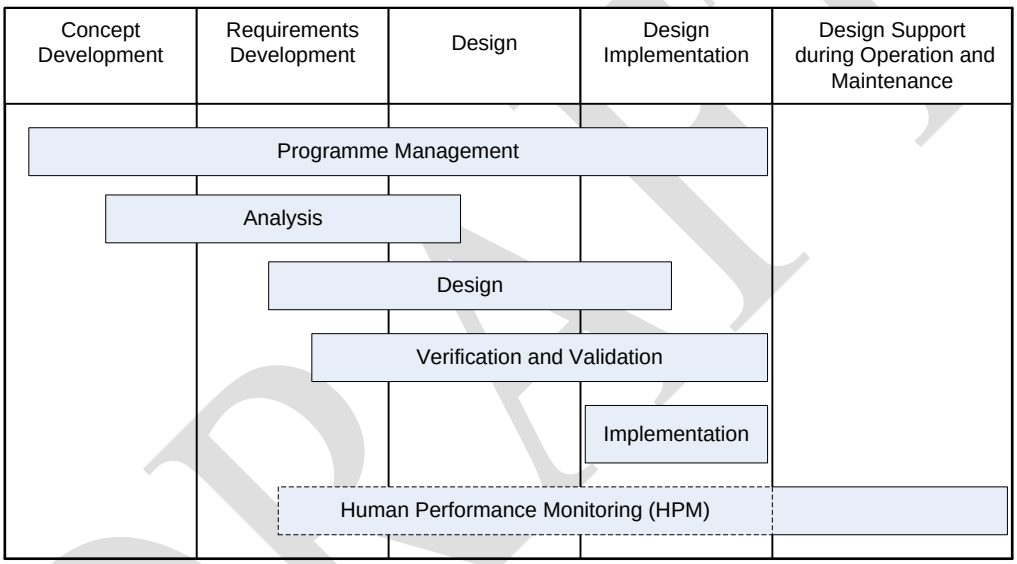

FIG. 1. An example of HFE generic process.

2.21. The following HFE inputs should be considered in the concept development phase:

— HFE programme management activities should identify a systematic, integrated HFE process, outline responsibilities for HFE and present expected design inputs and outputs for the HFE processes;

— HFE programme should establish a capable human factors organisation with sufficient authority on all hierarchy-levels to effect necessary design changes to meet the HFE expectations;

— HFE programme management should identify the most recent HFE relevant codes, standards, methodologies and guidelines applicable to the project;

— HFE analyses should identify relevant operating experience (both positive and negative) with a focus on human performance issues and potential human error and its mitigation;

— HFE analyses should provide inputs (such as operator needs and requirements) useful for defining and selecting relevant design choices;

— HFE analyses should help identifying the organizational architecture that frames the use of the HFE system, i.e. identification of users, their roles and responsibilities, required qualifications, regulatory requirements, and which support the developing concepts of operation and maintenance;

— HFE analyses should provide a preliminary understanding of function allocation, and human information requirements for monitoring and controlling (where applicable) functions of a system.

2.22. HFE analyses should provide insights and consideration how operators should respond in the presence of control system failures and HMI failures. The following HFE inputs should be considered in the requirements development phase:

— Results of the function analysis that identify functional requirements for the system;

— Results of task analyses, e.g. what kind of alarms, information, procedures, controls and system feedback are needed;

— Results of task analyses that provide insight into:

a) Possible sequence and flow of tasks;

b) Potential human errors as well as considerations that impact human performance and provide error reducing and performance enhancing design features;

c) Safety significant complex tasks that warrant detailed analyses and HFE evaluation;

d) Timeline constraints for significant tasks;

e) Specific knowledge, skills, and abilities needed by personnel in order to perform their assigned task(s) and meet operational objectives;

f) Collaboration and coordination between individuals or groups that are needed to support the task.

— Specific HFE design principles and HMI design guidelines for the development of vendor technical specifications, and for their incorporation into HFE vendor specification.

2.23. The following HFE inputs should be considered in the design phase:

— Updates to HFE requirements due to design evolution, and/or changes in standards;

— Specific HFE design principles and HMI design guidelines for the definition of facility / workspace design and layout, HMI components and their architecture;

— Specific HFE design principles and guidelines for maintenance and testing considerations;

— Potential impact of new or modified designs to human performance, procedure development and training;

— Collection and analysis of user feedback through early HFE evaluations in the form of prototype or concept usability testing and user review;

— 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 HFE inputs should apply to the design implementation phase:

— 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 has been provided in the design;

— HFE validation of the degree to which HMI design and supporting mechanisms facilitate the achievement of safe operation of the plant;

— Confirmation of the feasibility of human tasks identified as important to safety in the probabilistic and deterministic safety analyses through HFE validation;

— Confirmation of completion of HFE analyses and HFE input into design in accordance with HFE planning and regulatory expectations.

2.25. Throughout the design stages consideration should be made of constraints of the technology being considered, e.g. availability, reliability, band-with, and general acceptance and familiarity. For example, personnel accept the use of digital technology in everyday life; the designer may wish to consider whether virtual reality or augmented reality has the potential to cause issues for personnel.

2.26. Human performance monitoring in support of design should be conducted during operation and maintenance phases in order to verify that analyses and assumptions determined during the design phase remain valid throughout the plant life cycle.

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

2.28. HFE activities supporting 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 disciplines participating in the design.

2.29. HMI and its functionality should be treated from the perspective of HMI being part of an integrated whole and not as 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 that:

> "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. HFE should use the experience data and conclusions from event analyses as an input for design of the new plant or modification of operating plants.

3.3. The review of operating experience should provide information regarding current work practices for the following purposes: (a) to assess the potential impact of planned changes; (b) to evaluate operational problems and issues in current designs that may be addressed during plant modernization and modifications to plant components; and (c) to evaluate relevant industry experience with design options to instrumentation and control systems and HMI technology for their potential to improve plant efficiency and safety.

3.4. Operating experience review should analyse both positive and negative aspects of performance and design.

3.5. The operating experience review provides the following:

— Applicable HFE issues identified in review of plant operating experience;

— Issues identified from applicable predecessor designs;

— Experience insights identified by plant personnel;

— Operating experience from other nuclear power plants and industries.

3.6. HFE should consider operating experience data for any of the following:

— Minor problems that are often precursors or contributors to more significant events;

— Trends that detract from reliability;

— Existence of root cause data that could point to improvements in design;

— Evidence of culture influences and trends that could prove problematic for future operations;

— Corrective actions identification and implementation;

— Recurring events;

— Review of maintenance practices;

— Industry notices on best practices.

3.7. Ref. [7] provides recommendations on all the main components of systems for the feedback of operating experience, including gathering relevant information on events and abnormal conditions that have occurred at nuclear installations throughout the world.

FUNCTION ANALYSIS

3.8. Function analysis should provide a framework for understanding the role of personnel in controlling plant processes.

3.9. 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 defined and analysed.

3.10. Function analysis should help identify the information (e.g. the information when the function is needed, available, operating, achieving its purpose or terminating) and controls that personnel require accomplishing operational objectives.

3.11. Function analysis should also provide time and performance requirements and constraints for performing the functions.

3.12. Human, technology and organization factors should be considered when performing the function analysis.

3.13. Function analysis should help identifying high level acceptance criteria associated with maintaining safe operation of the plant.

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

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

— Relationships between high level functions and the plant's systems (e.g. plant configurations or success paths) responsible for performing the functions;

— Higher level functions should be decomposed into lower level functions that can be mapped to tasks to be performed by plant automation or the human, or human and automation jointly;

— A framework for determining the roles and responsibilities of personnel and automation.

3.15. The function analysis should document the combination of systems and processes used to achieve a high-level function and the human action required for success path.

3.16. The function analysis should document dependencies that may exist among plant functions, systems and their support systems.

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 defined and analysed.

3.18. Allocation of functions to human and machine should complement human capabilities (e.g. ability to improvise, flexibility, judgment, pattern detection) and machine strengths (e.g. rapidity, simultaneous processing of complex operations)

3.19. Human, technology and organization factors should be considered when performing the function allocation.

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

3.21. Allocation of functions make use of the analysis of plant control functions and lays out the allocation of control processes which may be assigned in the following way:

— Personnel, e.g. manual control (no automation);

— Automatic systems, e.g. fully automatic control, and passive, self-controlling phenomena;

— A combination of personnel and automation, for example:

  - Shared operation, the automatic operation of some aspects of a function, with others performed manually;
  - Operation by consent/delegation, automation takes control of a function when personnel have given permission and the situation permits;
  - Operate by exception, autonomous operation of a function, unless there are specific pre-defined situations or circumstances requiring manual human task.

3.22. In addition to consideration of human capabilities, when allocating functions, designers should also include such factors as technology readiness, time requirements associated with systems response, and considerations for defence in depth.

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

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

3.25. Allocation of functions should be analysed for different operational and accident scenarios.

3.26. Function requirements and allocation of functions should include requirements associated with

the implementation of severe accident management guidelines.

3.27. The allocation of function approach should be traceable from the function level to the system/component level.

TASK ANALYSIS

3.28. The task analysis approach should consider plant states and 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, technology and organization factors (e.g. leadership, management and communication) should be considered when performing the task analyses.

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

3.31. Task analysis should include the context of the task from the standpoint of user in order to accomplish the task.

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

— Tasks which are performed in different locations (e.g. control room, supplementary control room, field, technical support centres);

— Tasks which vary with the operational and accident scenarios;

— Tasks which require individual work and/or co-operation/exchanges between different disciplines (e.g. operation, maintenance, procedure development, computer system engineering) and interested parties;

— Tasks which must sometimes be performed under time pressure, harsh environmental conditions and context, or are extremely vital and rare.

3.33. When identifying the tasks, the following considerations to the risk and safety aspects may include:

— Tasks with occupational risk to the personnel;

— Tasks credited in the safety analysis report;

— Tasks identified as challenging or prone to error from operating experience;

— Tasks identified as difficult by operating personnel where no plans have been made to automate that task;

— Tasks, which are critical for maintaining the plant in a safe state or restoring it to this state following an event.

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

3.35. The results from this analysis should serve to identify the following:

— The expected human tasks and potential human errors which have an impact on safety;

— The expectations of how the task will be conducted, the expected task outcomes, and estimates of the reliability of human performance on the task;

— The error prevention factors in place for safety critical tasks;

— The impacted safety functions, initiating conditions and terminating conditions of each task;

— The order for implementing tasks and subtasks;

— The personnel needs (e.g. organizational aspects, staffing, qualification, training), the equipment needs (e.g. HMI elements, special tools and protective clothing), and documentation needs (e.g. procedures, processes, instructions);

— The human performance requirements and constraints (e.g. time, precision, independent verification);

— Required communication systems and access to those systems.

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

— Documentation (supplier documentation, technical specifications, existing procedures, manuals, training materials);

— Knowledgeable personnel from the design team, operating personnel who have gained operating experience in similar plants, stakeholders and experts;

— Walk–through and talk–through to analyse the predecessor system’s task activities and tasks from similar plants, as well as the tasks related to the system being developed;

— Data from the operating experience review (e.g. note differences from the reference design);

— Data from the customer requirements;

— Data from other analyses that are inputs to the HFE design process (e.g. functional requirements analysis and allocation, human reliability analysis);

— Data from other analyses that are inputs to the HFE design process (e.g. function analysis, requirements analysis, human reliability analysis, training needs analysis);

— Data from simulator studies;

— International HFE standards (see also Annex I).

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

3.38. The impact of task performance requirements 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. The task analysis is a collaborative activity and should involve a multidisciplinary team with HFE and operations expertise.

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

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

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

3.44. Table top analysis of documentation (e.g. procedures) alone may not be sufficient for determining that a task(s) can be performed. Stakeholder input and/or simulations supported by mockup, field walkdown, part task simulator, or full scope simulators may be performed to confirm the feasibility of the actions in real scenarios.

3.45. Task analysis should contain an error classification that at a minimum captures the errors of omission, errors of commission, including decision errors.

STAFFING, ORGANIZATION AND QUALIFICATION

3.46. Staffing, organization and qualification should be analysed for impacts on tasks important to safety that the required number of personnel, organizational interactions and qualification of personnel are sufficient for task performance.

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

— The safe completion of the operator tasks;

— The workload of the members of a team;

— The ability to synchronize the contribution of each team member to the task;

— The independence and coordination of the individuals responsible for checking (for example actions taken in the control room and locally by the operators);

— The perception of the task, its benefits, and its acceptability for the personnel.

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

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

3.50. The inputs of the staffing, organization and qualifications analysis should include:

— Concept of operation in normal operation and accident condition;

— Design requirements;

— Task requirements;

— Regulatory requirements;

— Operating experience;

— Human reliability analysis. (e.g. the human reliability analysis may determine that a two-person rule be in effect to reliable task completion).

3.51. The task analysis should be used in support of defining roles, requirements and responsibilities and required outputs of the work groups.

3.52. The following should be considered when assigning individual tasks to work group members:

— The tasks assigned to each member are clearly described;

— The basis for task distribution is determined and justified;

— The workload of each team member is reasonable in all operational and accident scenarios;

— The human performance impact is assessed when distributing the tasks between teams working day and night;

— The tasks required in various operating situations are assigned to work group members in order to ensure continuity of responsibilities and maintaining individual and collective 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. The important human tasks and actions should be identified from probabilistic or deterministic safety analysis.

3.55. The underlying approach to determining the important human tasks should consider operational

states including responses during accident conditions.

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

3.57. As a minimum, operator tasks and actions credited in the safety analysis, including relevant performance shaping factors should be analysed, and the ability for the design solution to achieve the necessary human performance related to safety requirements should be confirmed.

3.58. Regardless of which underlying approach is taken to identify important human tasks the HFE design, procedures, training, staffing level, and concept of operations should support the execution of important human decisions and actions.

3.59. Plant modification may alter the manner by which safety related tasks are executed and it should be assessed whether all associated safety related tasks can still be reliably executed.

4. HFE DESIGN

GENERAL HFE GUIDELINES

4.1. Requirement 32 of Ref. [1] states that:

> "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 Ref. [1] states that:

> "The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and limits 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 Ref. [1] states that:

> "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 a decision to act shall be simply and unambiguously presented."

4.4. The human machine interaction 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 needed.

4.5. The concept of defence in depth should be considered during HMI design 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 consider the human-centred approach which considers the equipment and systems from the perspectives of the personnel who would carry out functions and tasks associated with the design.

4.7. The human aspects, the machine (hardware and software), the work environment, and the control, operation and management should be considered during all phases of the design process (integrated, systemic approach).

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

4.9. Designers should consider the constraints and flexibility in the design to adopt different control or operational strategies across 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 to respond to a postulated initiating event;

— Whether HMI can support anticipation and response to an unexpected event;

— Whether HMI provides information on incremental changes in anticipation of sudden disruptions or fault conditions (e.g. predictive displays);

— Whether provisions and locations for additional tools and equipment are available;

— Whether utility implementation of ‘stress tests’ for plant systems in a presence of severe accidents may provide insights for how operators and responders may use equipment differently to possibly achieve safety functions;

— Whether implementation of different operational strategies may have to be adopted in order to achieve a safe state as an event unfolds;

— Whether equipment could be used out of its design function support, a different strategy (e.g. use of fire protection system to provide cooling).

HMI design inputs

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

— Operating experience review;

— Function analysis and function allocation;

— Task analysis;

— 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 sensor data availability);

— Physical environment;

— Cognitive limitations and strengths of the users;

— Knowledge, skills and abilities of personnel including various user/occupational types;

— Applicable regulatory requirements.

4.13. The HMI design should support the roles of operators in the plant, considering levels of automation identified in the processes of functional requirements analysis and function allocation.

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

— Tasks needed to control the plant during a range of operating conditions from normal through accident conditions;

— Detailed information and control requirements (e.g. requirements for display range, precision, accuracy, and units of measurement);

— Task support requirements including habitability (e.g. lighting and ventilation requirements).

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

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

4.17. This documentation should define the detailed design criteria for the HMI elements. In case of HMI modernizations in existing plant, it should be evaluated for any needed revisions based on the HMI modernization needs and concept of operation.

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

HMI detailed design and integration

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

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

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

4.22. The presentation of information should be integrated 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 control locations and platforms.

4.24. To the extent possible, the HMI should be designed to prevent and detect operator errors, where an action might be taken in an incorrect context, or with an inappropriate plant configuration. This includes validation of setpoint 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 where wrong information may be presented.

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

4.27. The human machine interface:

a) Should, as far as practicable, accommodate the different roles and responsibilities of various types of operating personnel expected to interact with the plant;

b) Should be designed with primary attention given to the role of the operator who is responsible for the safe operation of the equipment;

c) Should support the development of a common situational awareness on the part of the control room crew, e.g. via large wall–mounted plant status displays;

d) Should provide an effective overview of the plant status;

e) Should, as far as practicable, apply the simplest design from the users' perspective that is consistent with function and task requirements;

f) Should present information such that it can be rapidly recognized and understood by operators;

g) Should accommodate failure of analogue and video displays without significant interruption of control actions;

h) Should reflect consideration of human cognition, physiological characteristics, characteristics of human motor control and anthropometry.

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

4.29. The HMI, procedures and 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, test, and repair of the HMI without interfering with other plant control activities.

4.32. The HMI design should support personnel task performance under conditions of minimum, typical, and optimum staffing.

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

— Consistently with the design guidance used for existing ones, so that personnel have a similar interface across new and old equipment;

— Consistently 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. HMI design of local control stations should be consistent with HMI design in the control room.

4.36. The HMI design required for the supervisory control of safety systems should apply the principle 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 identified important human tasks.

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

HMI tests and evaluations

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

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

— Personnel–task requirements;

— Human performance capabilities and limitations;

— HMI system performance requirements;

— Inspection and testing needs;

— Maintenance demands;

— Use of proven technology and the operating experience of predecessor designs.

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

Design guidelines for the HMI controls

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

4.43. HMI controls may be implemented as soft controls, multiplexed or dedicated control devices and combinations thereof.

4.44. Analogue control devices (e.g. push button, rotary, slides, toggles, rocker switch) are suitable for controls in constant use, for example electrical output, or those whose immediate accessibility and reliability are of prime importance, for example an emergency trip button.

4.45. Controls should provide visual or auditory feedback within adequate time to indicate that the system has received a control input.

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

4.47. HMI should reduce the likelihood of unintended actuation by requiring deliberate action for their execution for actions that can have negative consequences (e.g. confirmation button, plastic cover over the switch).

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

— Locating controls at proper positions;

— Use of protective structures;

— Provision of a second confirmatory action;

— Use of interlocks or permissive signals, with proper assignment of priorities;

— Proper selection of physical characteristics, such as size, operating pressure or force, tactile, optical and/or acoustical feedback.

4.49. To minimize operator errors, control movements should conform to population stereotypes (e.g.

user expectation) and should be compatible with the controlled variable's attributes.

Design considerations for soft controls

4.50. Soft controls are implemented using video display units together with a pointing device (e.g. 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 using soft controls should include means for selecting the components to be controlled, the display areas where input is entered, and the formats used for entering data.

4.52. Interaction with soft controls should include 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 required;

— Information about the status of each component;

— Control the relationship to other components.

4.54. Selection displays show a set of components or variables to be controlled. Components and variables within selection displays 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 systems are discrete-adjustment interfaces, soft sliders and arrow buttons. Input formats for entering data should be provided in the soft controls.

4.57. The cursors should have a distinctive appearance; their movement should have a sensitivity compatibility with the required tasks and operators' skills. Their movement should conform to operators' stereotypes, 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 to the operator only available options and controls. The options should be listed in a menu added to the working display without requiring the operator to remember them or to access a separate menu display.

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

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

HFE design for workstations

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

— Workstation height;

— Benchboard slope, angle, and depth for consoles and sit-stand workstations;

— Control device location;

— Display device location;

— Layout of control and display devices at a console or workstation;

— Size of text and graphics for legibility;

— Clearances 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 or 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 be at a convenient height for operator visibility and legibility.

4.65. Frequently used controls should be within convenient reach and the related indicators and displays should be readable from the operating position.

4.66. Functional groups should be specified in terms of the achievement of a given function or process operation.

4.67. Types of grouping that may be used for building functional groups should be organized by function, by sequence of use, by frequency of use, by priority, by operating procedures or by system with mimic arrangement.

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

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

4.70. Controls, displays, and other equipment items located in workstations should be appropriately and clearly labelled to permit 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 content should describe the function of equipment items and the symbols 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 nomenclature used in procedures and that printed on the labels.

4.74. The workstation design should consider the test and maintenance operations which may have to be performed at the workstation. This should include:

— Access to the components on the panels for repair, removal, or replacement;

— Separation of controls and displays used only for test and maintenance from those used for operations;

— Contingency space for special test equipment or repairs.

HFE DESIGN FOR ACCESSIBILITY AND THE WORKING ENVIRONMENT

4.75. Paragraph 5.60 of Ref. [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 Ref. [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 where 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. Normal aspects of the working environment to be considered include lighting, temperature, humidity, noise and vibration.

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

4.80. One way of establishing suitable means of access is to provide a qualified route that should be protected against potential internal hazards or external hazards to supplementary control points and other field locations where operator actions are expected to occur.

MAIN CONTROL ROOM

4.81. Requirement 65 of Ref. [1] states:

> "A control room should 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 Ref. [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 Ref. [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."

HMI design guidelines for the main control room

4.84. A control room design should be consistent with the concept of operation, which should describe how the plant will be operated in all plant states.

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

— Operational goals and objectives including safe operations;

— Organization of HMIs into workstations (e.g. consoles and panels);

— 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. Control room design should consider the display options that would provide a high-level summary of plant status and support crew coordination on shared tasks and awareness of each other's activities.

4.88. Display devices should be provided in the main control room in order to allow operators and supervisors to monitor all functions important to safety, 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, abbreviations, should be identifiable and readable from the maximum task specific viewing distance under minimal ambient lighting conditions.

4.90. The display system should communicate the intended information to the operator without ambiguity or loss of meaning, 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. Numeric values should be displayed only to the level of significance required of the data for operation, regardless of higher levels of significance of individual input data.

4.93. Display system response time 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 those of another of higher priority.

4.95. HMI design should consider where common or coordinated actions are to be made by the operators.

4.96. HMI information should allow operators to immediately assess overall plant status and detect conditions that require attention without performing interface management tasks.

4.97. Information shown on video display units should be clearly understood 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 and its values are operating properly (or that a system failure has occurred).

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

4.101. HMI for real time tasks requiring fast operator response should require limited operator

actions. For example, limit travel distance for cursors across and between display pages, scanning time and the number of windows on a display.

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

4.103. Operators should be able to request guidance information regarding requirements for information of command entry (e.g. syntax, parameters and options).

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

4.105. A standard display screen organization should be evident for the location of various HMI functions (such as a data display zone, control zone or message zone) from one display to another.

4.106. The HMI display system should clearly indicate which items are selectable. When the operator is performing an operation on some selected display item, this item should be highlighted in order to avoid errors.

4.107. HMI should be user friendly, without requiring the operator to memorize special additional and varying codes or sequences to perform translations and conversions.

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

Main control room layout

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 conditions.

4.110. Main control room staffing and task assignments should ensure complete and timely coverage of controls, displays, and other equipment required during all modes of operation.

4.111. Layout of desks and consoles in the main control room:

— Should permit full view of all control and display panels (including alarm displays);

— Should facilitate voice communications from operators at the workstations to any point in the main operating area;

— Should permit access to workstations without having 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. These places should permit an easy access and extraction of documents.

4.113. A storage space of emergency equipment that control room personnel may require during accident conditions should be provided with ease of access.

Habitability considerations

4.114. The main control room should provide an environment under which the main control room staff are able to perform their tasks without discomfort, excessive stress, or physical hazard.

4.115. Workspace design of the main control room should consider environmental factors that can have an important effect on personnel performance including designing for thermal comfort, illumination including emergency scenarios, auditory environments that promote clear verbal communications, and facility layout.

4.116. The control room should contain sufficient facilities and supplies to ensure comfortable sustained occupancy during response to design extension conditions.

4.117. The control room design should include assessment and protection against missiles originating from outside the control room. Guidance on the protection from missiles is provided in Ref. [8].

Design guidelines for the HMI of the safety parameter display system

4.118. The safety parameter display system (SPDS) should be provided to aid the main control room personnel during accident conditions in determining the safety status of the plant and in evaluating whether conditions require corrective actions by operators to avoid a degraded reactor core or release of radioactivity.

4.119. The SPDS design should incorporate HFE in order to enhance the functional effectiveness of main control room personnel.

4.120. The SPDS should provide information on the critical safety functions associated with the reactor design.

4.121. The SPDS should be located conveniently for the main control room personnel and provide continuous display information from which the plant safety status can be readily and reliably assessed.

4.122. The SPDS should be designed to bring together a minimum set of plant parameters from which the operator can assess the plant safety status without surveying the main control room.

4.123. The devices used to display SPDS information may include analogue and computer-based devices. Analogue display devices could be meters, light indicators, numeric readouts and plotters. Computer-based display devices could be flat panel devices and large screen devices.

4.124. The SPDS display devices should conform to the main control room HMI general design guidelines.

4.125. The SPDS should be consistent and compatible with other displays and devices of the HMI for presenting and coding information.

SUPPLEMENTARY CONTROL ROOM

4.126. Requirement 66 of Ref. [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 consider HFE principles and human characteristics of personnel under emergency conditions, particularly for immediate actions.

4.129. Means should be provided to ensure habitability of the supplementary control room also in case that long term occupation is required (e.g. equipping ventilation systems with backup power supply and filters such as iodine).

4.130. Workspace design of the supplementary control room should consider environmental factors that can have an important effect on personnel performance including designing for thermal comfort, illumination including emergency scenarios, auditory environments that ensure verbal communications, and facility layout.

4.131. Computer based information or controls used at the supplementary control room should function in a manner closely matching and preferably in an identical way to that of similar controls and indications in the main control room.

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

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

4.134. Communication between the supplementary control room and local control points, with the plant management, external crisis management groups and the technical support centre should be provided.

EMERGENCY RESPONSE FACILITIES ON THE SITE

4.135. HFE should be applied when designing emergency response facilities [1] including site technical support centres. The design should provide for optimal layout of individual workplaces, and data and information needed to perform the activities required for the implementation of accident management strategies.

4.136. Displays in emergency response facilities supporting situation awareness should be designed through application of accepted HFE methods and principles. These include illumination, size, geometry, display and control layouts, available content, suitable format and standardization of the displays, and fundamentally consider the task to be performed with the information provided by the display.

4.137. Operating experience reviews, 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. HFE should consider resource allocation strategies (e.g. staffing), the physical conditions of a facility (e.g. power supply, accessibility, 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 should be considered when personnel are required to operate the non-permanent accident mitigation equipment credited during severe accident management. This includes safe access to local controls to enable the safe use of non-permanent equipment. Typical examples for local controls include local control panels, connection points, switches, terminals, etc. that (a) enable connection of non-permanent equipment, or (b) enable operation of equipment (e.g. pumps) for which non-permanent equipment provides electricity.

4.140. HFE should consider the range of internal and external interaction of individuals and interested parties at all levels with the on-site and off-site emergency response organization under emergency conditions.

4.141. HFE should consider the level of stress and workload that can exist during emergency response operations.

[1] Emergency response facilities are addressed in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency, Ref.[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.

4.142. The technical support centre staff should be trained on the identification and use of the instruments to support implementation of severe accident management guidelines. More detailed recommendations for the development and implementation of severe accident management guidelines are provided in Ref. [10].

ALARM MANAGEMENT

4.143. Paragraph 5.66 of Ref. [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 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 or rate of change deviations from control or protection setpoints;

— 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 expected system response should be assimilated to status information.

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

4.148. The system should have a sufficient coverage for operational states and accident conditions.

4.149. Paragraph 7.9. of Ref. [2] requires that the number of alarms is 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. Alarmed states can be selected among the different states of the signal (e.g. on/off, open/closed, tripped/untripped).

4.152. Generated alarms should support an alarm hierarchy consistent with the structured architecture of the plant.

4.153. Alarm generation should be context-aware (e.g. pump low flow alarms generated on 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 generation of unneeded momentary or chattering alarms.

4.155. Alarm systems should be able to reduce automatically the number of alarm conditions at the signal level.

4.156. Alarm systems should support alarm inhibition to avoid alarms occurring as nuisances or becoming standing alarms.

4.157. Alarm inhibition takes inactive alarms out of service by disabling alarm generation, normally during testing, maintenance or repair of the associated equipment.

4.158. HFE analysis and validation should determine whether one alarm is masking the occurrence of another alarm(s).

4.159. Alarm systems should support alarm prioritization to determine the relative importance between alarms.

Alarm processing

4.160. The alarm system should support user–defined alarm generation. 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.

4.161. Alarm systems should be able to apply event–based and significance–based fundamental alarm suppression techniques at different hierarchy levels:

— Event–based reduction techniques filter/suppress alarms generated as a consequence of a support equipment/system failure or a plant event;

— Significance–based reduction techniques suppress lower-priority alarms in situations with alarm overload.

4.162. 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

4.163. The alarm system should provide visual indications when any alarm condition appears or clears. Visual indications may 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 one has already occurred and has been acknowledged;

— Colour coding, alarms can light with different colours depending on the alarm priority, on the alarm state. Other display coding methods may be used.

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

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

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

Alarm presentation

4.167. The dark–board criterion consists of minimizing the number of alarms presented during normal operating conditions without challenging plant safety.

4.168. Alarm processing should follow the dark-board criterion at full power and recommended at other normal operating conditions.

4.169. Alarm presentation should be based on following different types of displays:

— Spatially dedicated continuously visible displays (e.g. analogue tile panels or arrays of visual display units with continuously visible tile-like panels, 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, resulting from the combination of the other types of displays.

4.170. Information about state changes and alarms should be presented and managed separately.

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

4.172. Alarm messages should contain all the information the operators need to respond to them effectively, such as alarm sources, priorities, descriptions, setpoints and parameter values, and

references to alarm response procedures and associated displays.

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

— Chronological order;

— Priority levels;

— Alarm status;

— Tag identity;

— Any other logical order.

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

4.175. Individual alarm information displays should be used to provide specific information of 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 related to the alarm.

Alarm response procedures

4.176. Paragraph 7.9 of Ref. [2] requires that alarm response procedures are established for all alarm panels in the control rooms.

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

— The system/functional group to which the alarm belongs;

— The exact alarm message;

— Alarm priorities;

— Automatic, immediate and other operator actions;

— A list with the potential cause(s) for the alarm;

— References.

PROCEDURE DEVELOPMENT

4.178. Guidance in this section provides recommendations on human factors aspects of procedure development in support of Ref. [11][10].

4.179. Important human tasks identified by safety analyses, should be covered in procedures.

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

— Availability and status of equipment needed to successfully complete procedure;

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

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

4.182. Procedure development should also consider inputs from task analyses to:

— Identify potential errors that should be highlighted in the procedure;

— Provide required flow of information, actions, and feedback necessary for successful completion of a task;

— Identify links between tasks and personnel;

— Provide preliminary timing information;

— Transition between procedures;

— Format and content of technical warnings, pre-requisites (initiating conditions) and procedure termination.

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

4.184. HFE design input to development of plant procedures should consider format and content that is commensurate of the category of procedure (e.g. emergency operating procedure, maintenance and test procedures).

4.185. Safety critical tasks, complex tasks, and rarely performed tasks should be detailed step by step.

4.186. The procedure should provide guidance for safe contingent actions if the actions specified cannot be achieved or guidance for terminating the procedure safely.

TRAINING PROGRAMME DEVELOPMENT

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

4.188. 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

display representation.

4.189. 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.

4.190. The training plan should be reviewed and modified periodically according to the evolutions of HFE design.

4.191. Training should be timely, and training associated with modifications or modernizations, of HFE design should be completed prior to operation.

4.192. The development of a training programme should follow the guidance provided in Ref. [12].

5. HUMAN FACTORS VERIFICATION AND VALIDATION

GENERAL

5.1. The human factors verification and validation should comprehensively determine that the HMI system conforms to specified HFE design requirements and that 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, simulations that become increasingly realistic as the project progresses.

5.3. Verification and validation should be performed by persons or parties independent of the design.

5.4. Verification and validation should provide objective evidence that HFE designers have adhered correctly to design principles and requirements for usability when the human, technical and organizational aspects are combined.

5.5. Verification objectives typically include:

— Identification of HFE standards and guidelines;

— Verification of the HMI includes hardware (e.g. consoles, panels, analogue interfaces, including alarm displays), the software, and associated documentation (e.g. procedures, instructions, alarm sheets);

— Review of design requirements, drawings, manuals;

— Verification of task support includes the provision of tools, job aids, personal protective equipment, task-related equipment, training, qualifications of operators, and accessible and usable procedures at the point of need.

5.6. Verification activities may include interactions with system users. Validation activities necessarily include user representatives who are independent from the design team.

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

— The ability of the crew to complete the required actions in operational states and accidents conditions;

— The presentation and the organization of procedures to support task performance;

— The human system interface as it supports operator tasks;

— The layout of the work space 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 control room HFE design should include:

— The layout for the main and supplementary control rooms supports the operators' tasks;

— The effectiveness of measures relating to monitoring, control and maintenance (in and outside the control rooms);

— The monitoring and control systems in the control room linked to the entire installation that is used by the personnel in all operating states and accident conditions.

5.9. A validation of the integrated system of hardware, software, procedures, and humans should be performed before the HFE 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 are implemented beforehand, in particular:

— The operating concept in all operational and accident conditions;

— The technical and user requirements of the tasks especially that are safety sensitive;

— The functional and detailed specifications of the means of control, of the level of automation;

— Inputs from functional analysis;

— The regulatory requirements;

— Input from operational feedback;

— Human tasks that are important for safety;

— Data from safety analysis;

— Data from human reliability analysis;

— Data on staffing, organization, and qualifications;

— Data from previous human factors engineering reviews and analyses;

— Input from simulation where available (e.g. may include part-task simulation).

VERIFICATION AND VALIDATION PLANNING

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

5.12. Verification and validation planning is an iterative activity that supports project changes as design progresses, for example:

— More interfaces become available;

— Procedures are more detailed;

— Operators are trained;

— Simulations fidelity becomes realistic.

5.13. The verification and validation planning should specify:

— Scope of the evaluation;

— Data collection and analysis;

— Measures of effectiveness;

— Evaluation and acceptance criteria;

— Participants involved in the evaluation;

— Training requirements for the evaluation team including for those participating as user representatives;

— Test environment;

— Schedule.

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

— Scenario selection;

— Participants (i.e. user selection) and their training;

— Materials[2] and tools used by the evaluation team.

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

— With the project's HFE requirements (e.g. ergonomic requirements and project specific requirements);

[2] Materials are all the elements used by the validation team e.g. audio, video, computer recording, questionnaire.

— With the plant operational acceptance criteria;

— With 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 issues;

— The tracking of the HFE 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 installation, instructors, experts in operations in the event of incidents and accidents, HFE experts).

5.18. The validation tests should be conducted by participants organised in accordance with the organizational layout for the future operation.

5.19. The participants in the validation test 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, HFE verification and validation should include all or a subset of the following.

— Static test (e.g. meets the design specifications);

— Dynamic test (e.g. system response in terms of time and accuracy);

— Scenario testing and part task or full scope simulation (e.g. operator response in terms of time and accuracy);

— Observation;

— Self-report (e.g. questionnaire, structured interviews);

— HFE check list (e.g. within static or dynamic test);

— Walkthrough.

5.22. The test participants should be familiar with the relevant portions of the modifications beforehand.

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

PERFORMANCE MEASURES

5.24. HFE verification and validation should apply relevant human performance measures for the

actual work environment. These measurements may include:

— Complexity of task to be performed;

— Workload (e.g. individual and team);

— Knowledge, skills, and abilities required with respect to the design;

— Sequencing and response times;

— Requirements for situation awareness (e.g. individual and team);

— Requirements for procedure usage;

— Requirements for detecting and responding to adverse conditions;

— Requirements for collaboration and communication between users and with other work groups.

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

— Time;

— Accuracy;

— Communication frequency and content;

— Error detection and error recovery;

— Situation awareness parameters (e.g. cue identification, comprehension, prediction);

— Use of group decision-making methods;

— Gaze and dwell time (e.g. from eye tracking methods);

— 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 used in the review depends upon 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. time constraints, sequence, precision).

VALIDATION TESTING

5.28. The test scenarios chosen to validate the HFE design should be realistic to the extent possible, including:

— Simulation and test bed should correspond to the design and physical layout;

— The tested scenarios should be representative of the operating conditions during all plant states and should include events (e.g. failures) to occur and their initiating conditions;

— The operating tasks (e.g. monitoring, detection, diagnosis, anticipation of changes in parameters, surveillance, control, manual recovery of automatic control systems);

— The participants should be trained and should occupy a position corresponding to their levels of qualification and responsibility;

— The procedures applied should match those that will be used in the relevant operating conditions;

— Range of human interactions expected during scenarios.

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 a HFE V&V plan. That plan should specify the duration or number of trials for data test, the systems and subsystem HMI to be tested, and the number of subjects from which data are to be collected.

5.31. Data collection should be deployed in the course of the tests on mockup, field part task simulator, or full scope simulators in order to detect, for example:

— The actions taken by the test participants (e.g. manual collection 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 the crisis management.

5.32. The means of collecting data during the tests should be used to collect deficiencies, i.e. the detected difficulties and mistakes made by the test participants and, on the other hand, to collect data on the ease of use when using the tools anticipated by the design. Consequently, the validation tests should 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 installation and the understanding of the situation;

— To optimise the workload of the personnel;

— To encourage coordination and communications amongst the personnel.

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

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

— The chronology of the actions;

— The identification of tasks that were performed consistently well and without issues;

— The identification and analysis of remarkable facts in the execution of the scenario (e.g. any difficulties encountered by the personnel, hesitations about how to proceed, misunderstandings between the members of the control room team about the status of the systems or the equipment).

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

DATA ANALYSIS

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

— 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 (e.g. made by analyst and users).

5.37. The analysis of the collected data should justify 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 are able to:

— Comprehend the situation;

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

— Coordinate with one another in the control room, and with the personnel with which the control room personnel has to interact (maintenance personnel, automatic control systems personnel, crisis management teams).

5.38. The HFE issues should be systematically documented and tracked.

5.39. The corresponding mitigation solutions and their effectiveness should be documented, evaluated and monitored.

5.40. The data collected in each test campaign and its 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 performed verification and validation 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 must be validated on site after the installation enters operation, should be specified.

6. HFE DESIGN IMPLEMENTATION

6.1. The HFE design implementation phase comprises the development, deployment and evaluation of the output from the HFE design process.

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

6.3. The HFE design implementation phase should evaluate whether the as–built design conforms to the verified and validated design, and if there are any unforeseen issues that arise when the design is implemented in the actual plant and work environment.

6.4. The HFE design implementation phase should confirm that:

— The implementation of the HFE design process matches its technical specification in terms of standards, functionality, and safety performance;

— The implemented HFE design has not generated any issues or conflicts (e.g. safety, operability or cultural) relating to personnel, safety management systems, technological systems, structures or components (e.g. inconsistencies with existing systems or interfaces).

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

— Organisation factors;

— Personnel factors;

— Job design;

— Safety analysis;

— Probabilistic safety assessment / human reliability analysis;

— Human machine interface;

— Equipment;

— Procedures;

— Training;

— Plant reference documentation;

— Working environment.

6.6. The HFE design implementation phase should give appropriate consideration to the following aspects:

— An assessment, which considers the consequences of the as–built design on actions that might be required to mitigate any undesirable consequences from implementing the HFE design;

— Elements that need to be in place prior to commencing the implementation e.g. simulator or test rigs training which is necessary to attain the desired level of task performance from the implementation team;

— A definition of criteria for successful implementation. This may link to the human performance monitoring system to ensure that the right things are being tested / measured;

— A method for capturing, assessing and resolving HFE issues that are identified during the implementation phase;

— Where practicable, contingency strategies in the event that the implementation fails to deliver against its performance objectives.

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

— Evidence that the outputs of the design project, including support provisions (e.g. HMIs, procedures, training) meets the relevant standards, performance, and success criteria, defined for it at the start of the project;

— Any negative effects on the human, technology and organisation are tolerable or suitably ameliorated;

— Any changes made to as–built HFE design are reflected in plant drawings and material, e.g. training material, procedures, drawings, simulators, organisational structures, and ancillary equipment;

— All HFE related issues in the issue tracking system have been adequately addressed;

— Any new HFE design related issues have been captured and assessed, and a suitable route to resolution assigned;

— Any remaining non–conformances have been assessed and deemed to be acceptable on safety grounds.

7. HUMAN PERFORMANCE MONITORING

7.1. The monitoring of human performance should be an active and on-going process to evaluate the continuing effectiveness of the design to properly support people to carry out their work tasks safely and effectively. It provides insight into:

— Whether the HMI design meets (and continues 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 within time response and performance criteria;

— Whether the level of performance established during the system validation is maintained over the plant life;

— Whether the system support such as supervision, training, staffing, procedures, personal protective equipment, tools and job aids are appropriate and sufficient to support the people performing their tasks.

7.2. Human performance monitoring should consider the following:

— Those responsible for human performance monitoring and the users of its outputs are adequately trained;

— Those responsible for human performance monitoring are suitably qualified and experienced in the domains of human and organizational factors, systemic approaches, and root cause analysis methods;

— Whether the causes and significance of deficient human performance are comprehensively understood and the means for performance improvement are identified;

— The effective use of issue reporting by system users in monitoring human performance needs a culture of open and honest reporting;

— Individual and team performance is directly affected by all levels within the organisation and therefore effective human performance monitoring should capture data from all levels;

— A sufficient flexibility is applied proportionate to the risk presented by the deviation in acceptable human performance;

— Progress in responding to and resolving degraded human performance is monitored to ensure that the response is within appropriate timescales.

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

7.4. Where applicable, the human performance monitoring should be compatible with new build projects where the owner/operator is not the design authority. This is to ensure that assumptions made during the design phase about human performance are captured and validated during the licensing and operational phases.

8. HFE DESIGN FOR COMPUTERIZED PROCEDURES

GENERAL

8.1. The computerized procedures may 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 that provides different levels of functionality including varying levels of automation.

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

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

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 procedure 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 included embedded soft controls to manipulate plant equipment. These systems may include the capability for automated sequences of steps that automatically carry out the described actions in the procedure.

GUIDELINES FOR COMPUTERIZED PROCEDURES SYSTEM´S HMI

8.6. HFE should be applied into the design of computerized procedures for both new and currently operating plants.

8.7. The following HFE principles should apply to computerized procedures:

— Display as reasonably achievable only relevant information for the task to be done;

— Continuously provide distinguishing information, e.g. title, revision number, date, plant name, 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 procedure system;

— Arrange computerized procedures system (including e.g. structure, format, navigation menus, 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 needed to correctly carry out the procedure.

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

INTERACTION WITH THE COMPUTERIZED PROCEDURES SYSTEM

8.10. The following interaction capabilities are applicable to computerized procedures Type I, II and III, unless otherwise is specified.

8.11. Warnings and cautions referred to 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;

— Every warning or caution is presented in a way that is easily distinguished from other cautions or warnings.

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

— It makes it easy for the operator to process the information;

— This group of items is clearly distinguished from other set of items;

— It includes a header specifying the content of the list.

8.13. Status of the steps of a procedure (e.g. specifying 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. Also an indication of alternative action where necessary should be included

8.14. For Type II and III computerized procedures the system should record and store the progress through the procedure.

8.15. The computerized procedures system may have multiple procedures being executed at the same time.

8.16. In such instances, human resources are allocated appropriately and coordination of the execution of multiple procedures should be considered. For example, when more than one procedure is being carried out simultaneously with another, the procedure and progress in that procedure should be displayed at all devices.

8.17. The computerized procedures system should include a navigation support that allows the operator to move within the procedure (between steps or other parts in the same procedure) and from one procedure to another (e.g. through active links).

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

8.19. Data and logic rules evaluated by the computerized procedure system should be available to the operator.

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

8.21. Operators should be in charge of deciding which procedure needs to be used according to plant status. Computerized procedures system may suggest what procedure to use but responsibility for this decision lies with the operators. This applies to computerized procedures Type II and III.

COMPUTERIZED PROCEDURES SYSTEM FUNCTIONAL CAPABILITIES

8.22. The computerized procedures system should notify the user when plant conditions necessitate proceeding to enter, exit or transition from one procedure to another.

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

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

8.25. The computerized procedures system may automatically process step logic (e.g. step succession) and provide this information to the operator. Results of the step logic should be highlighted.

8.26. The computerized procedures system should indicate those steps that need continuous monitoring. These may be time–dependent and process-dependent steps that are monitored by the operator.

8.27. The system should alert the operator when expected conditions in these steps are reached.

8.28. In addition, the computerized procedures system should indicate whether parameter monitoring has stopped or still being continued.

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

DEGRADATION AND FAILURES OF THE COMPUTERIZED PROCEDURES SYSTEM

8.30. HFE should develop guidelines for switching to backup procedures (e.g. paper, and/or backup hardware panels), as well as for switching back from back-up procedures to the computerized procedures when it works again

8.31. Degraded conditions and failures requiring a transition to a backup procedure should be recognized and indicated by the computerized procedures system.

8.32. Paper based procedures used as backup procedures should be available and accessible.

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

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

— Procedures which were currently being carried out;

— Procedure steps already completed and those not completed, including the step in which the execution was interrupted;

— Information about continuously monitoring steps or condition that were being monitored when the transition took place;

— Information needed to continue the execution of the procedure where it was interrupted, avoiding repetition of steps already completed.

8.35. Time needed to transition to back up procedures should be validated as meeting system functional requirements.

8.36. Computerized procedures training should include specific steps required for transition to paper based procedures.

AUTOMATIC SEQUENCE OF STEPS IN COMPUTERIZED PROCEDURES

8.37. Highest level of computerized procedures is automatization, i.e. automated sequences of steps that automatically carry out the described actions in the procedure. Automation of the sequences of procedure steps is only applicable to procedures Type III.

8.38. Automated sequences present in computerized procedures should be authorized and monitored by operators, who are responsible for safe plant operation.

8.39. Operators should be able to choose either to execute the steps of the procedure manually or activate the automation.

8.40. Operators should be in charge of selecting which procedure will be used.

8.41. Automated sequences of steps should be included (begin and end) in one single procedure.

8.42. Detailed and specific sequence should be indicated by the computerized procedures system.

8.43. Information about the progress of the automated process should also be provided (completed, current and pending steps).

8.44. Failures of automation should be indicated along with the point in the sequence when failure occurred.

8.45. Information about necessary initial conditions to be satisfied before executing an automated sequence of steps should be indicated by the computerized procedures system.

Hold points in automated sequence

8.46. An automated sequence of steps may include a hold point, which is a predefined point in the procedure at which the procedure needs the operator to acknowledge the status of the automated sequence and to authorize the procedure to continue.

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

— Help the operator to recognize the progress of the automation and to make any relevant and necessary decision/ adjustment for the procedure to continue;

— Keep the operator conscious of the status of plant equipment involved in the sequence of steps being carried out;

— Enable the operator to authorize the procedure to continue.

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

8.49. Predefined hold points should not be allowed to be removed by the operator.

8.50. 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 sequence

8.51. The computerized procedures system should allow the operator either safe transition from automatic to manual execution or to resume automatic execution.

8.52. Information about the interruption such as why the sequence has been interrupted, what steps have been completed and which ones are still pending to be executed should be provided by the computerized procedures system.

8.53. Computerized procedures system should be able to automatically interrupt an automated

sequence in the event that a needed condition for the step to be completed is not met, or there is any other situation that may not guarantee the safe completion of the current step.

8.54. Computerized procedures system should alert the operator of any interruption of the procedure.

9. HFE INTEGRATION IN SAFETY PROCESSES

DEVELOPMENT AND REVIEW OF SAFETY ANALYSIS REPORT

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

9.2. HFE considerations present in the safety analysis report should cover at minimum the following:

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

— The human factors analysis methods applied;

— Assumptions for the choice of HMI design taking into account HFE;

— Human factors verification and validation, including identification and resolution of HFE issues identified during the design project and assumptions made during analysis;

— A description of how HMI design has been implemented in the overall plant design;

— A description of human performance monitoring strategy for safety critical tasks.

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

9.4. HFE analysis should be considered whenever manual actions are credited to backup automatic actions in the design analysis as part of diversity.

9.5. Modernizations and modifications of HFE design should be documented in the safety analysis report.

9.6. Guidance on the format and content of the safety analysis report is given in Ref. [13].

PLANT MODIFICATIONS AND MODERNIZATIONS

9.7. Paragraph 4.40 of SSR 2/2 (Rev. 1) [2] states that:

> "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. HFE review should be conducted whenever modification of human tasks results from modernizations, small or large, to identify a potential risk impact.

9.9. HFE should be conducted whenever changes (sequencing, timing, and workload) are made to

procedures for which credit is taken in the safety analysis.

9.10. The effect of the plant modification and modernization on human tasks should be reviewed.

9.11. The HFE programme on plant modification and modernization should use a graded approach.

9.12. Any modification and modernization involving HFE solutions should be transferred to plant controls before being put in operation (e.g. documentation, procedures, layout, administrative controls, training).

9.13. Guidance and recommendations on controlling activities relating to modifications at nuclear power plants are provided in Ref. [14].

PERIODIC SAFETY REVIEW PROCESS

9.14. The clauses in this section provide guidance on HFE activities that can support the intent of Ref. [15].

9.15. The periodic safety review should confirm whether the following continue to be valid:

— The most resource intensive conditions feasible in each operational mode / plant state;

— The division and coordination of work in the most resource intensive conditions is feasible, through assessing function allocation, task analyses, and workload analyses.

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

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

9.18. The periodic safety review should consider whether the expectations of staff competencies align with human limitations and capabilities, task requirements, and regulatory requirements.

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

10. HFE IN PRODUCT SELECTION AND PROCUREMENT

10.1. The following section provides a consideration of relevant 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 severe accident mitigation equipment), commercial off the shelf products and mobile devices (e.g. hand held, portable, and wearable).

USE OF PERSONAL PROTECTIVE EQUIPMENT

10.2. Personal protective equipment and their characteristics should be selected and be compatible with the users' anthropometry, the tasks 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 systems, tools and job aids that may be used while wearing it.

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

10.4. HFE analysis should determine that the task can be carried out whilst using protective equipment, which may affect the users' vision, hearing dexterity, mobility and abilities to work in extreme temperatures.

10.5. Personal protective equipment should be verified and validated related to their intended use across various plant conditions (e.g. during drills and emergency exercises). This verification and validation needs to consider the full range of body sizes of the user population to be accommodated.

COMMERCIAL OFF THE SHELF PRODUCTS

10.6. Where commercial off the shelf (COTS) products are integrated into an existing system, HFE considerations should be given to selecting those ones that are consistent with the plant's design, operation, and maintenance philosophy.

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

— Within a system;

— Between similar systems that workers already interface with;

— With existing station conventions for HMI characteristics.

10.8. Where a COTS product is integrated with an existing system, the impact on human performance should be assessed.

10.9. HFE should ensure that the installation of a COTS product does not result in undesirable changes in the work environment or in the way that tasks are performed.

10.10. HFE should determine whether the COTS product requires additional training, modified or new procedures, maintenance or testing, or change in skills and qualification requirements.

MOBILE DEVICES

10.11. The HFE review of mobile devices includes hand held, portable, and wearable devices.

10.12. Selection of mobile devices should be based upon analyses that reveal the mobile device is appropriate for the task and the length of time that users should be able to hold, interact with,

transport, or wear the device. The mobile device should be also appropriate for the task if the personnel are wearing personal protective equipment.

10.13. Mobile devices and their characteristics should be selected and be compatible with the users' anthropometry, environmental conditions and HFE design criteria, e.g. for lighting, grip, size and weight.

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

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

10.16. Storage of the hand held mobile devices should be considered in HFE evaluations.

10.17. HFE should consider requirements for synchronization or calibration of mobile devices that may be unique to this form of interface.

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

— Error correction functions (e.g. where users are required to make entries into a system, an easy means to be provided for correcting erroneous entries, correction of individual errors without requiring re–entry of correctly entered commands or data elements);

— Features for user and software early detection and correction of errors after keying in, but before entering into the system;

— Error checking such as at the end of data fields rather than character–by–character, in order to avoid disrupting the user;

— User control of the process when controlling equipment from a mobile device (e.g. 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 radiated fields should be considered and 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, A System for the Feedback of Experience from Events in Nuclear Installations, IAEA Safety Standards Series No. NS-G-2.11, [[DS479]], IAEA, Vienna (in preparation).

[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) [under revision by DS494].

[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 NUCLEARTEST-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, Vienna (2015).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna (2009) [under revision by DS483].

[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).

[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).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Format and Content of the Safety Analysis Report for Nuclear Power Plants, IAEA Safety Standards Series No. GS-G-4.1, [[DS449]], 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).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-25, IAEA, Vienna (2013).

ANNEX I

BIBLIOGRAPHY OF INTERNATIONAL I&C AND HFE STANDARDS

I–1. Requirement 9 of SSR 2/1 (Rev. 1) [I-1] states:

> "Items important to safety for a nuclear power plant should be designed in accordance with the relevant national codes and standards."

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

I–3. Two standards development organizations are responsible for most of the internationally used standards for instrumentation and control systems in nuclear power plants: the International Electrotechnical Commission's (IEC) Subcommittee 45 (SC45A) and the Institute for Electrical and Electronic Engineers' (IEEE) Nuclear Power Engineering Committee (NPEC). Each organization has developed a large number of standards. Both organizations produce standards that respond to the common principles underlying the requirements of Ref. [I–1] and the recommendations of this guide. Consequently, either set of standards can be used to further interpret the recommendations of this Safety Guide.

I–4. This annex is intended to help readers understand the relationship between this Safety Guide and the IEEE and IEC standards. Table I–1 lists the IEC and IEEE standards that have a strong relationship with the recommendations of this Safety Guide. Table I–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.

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

I–4. A concerted effort was made to avoid conflicts between the recommendations of this Safety Guide and the standards of IEEE and IEC. 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.

I–5. Nevertheless, users need to recognize and take account of the fact that there are important differences between the IEC and the IEEE standards.

I–6. IEC standards take the IAEA Safety Requirements and Safety Guides as fundamental inputs for the development of their standards. 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.

I–7. IEEE standards focus largely on safety items and, therefore, their guidance directly applies to a smaller set of functions, systems and equipment than this Safety Guide does. Nevertheless, the guidance of IEEE can be applied to safety related items (items important to safety that are not safety systems) using a graded approach.

I–8. Other guidance documents, e.g. NUREG–series publications involve reports or brochures on regulatory decisions, results of research, results of incident investigations, and other technical and administrative information. These guidance documents relate to the major topic areas of this Safety Guide as well. Table I–2 shows how other guidance documents relate to the major topic areas of this Safety Guide.

TABLE I–1 INTERNATIONAL STANDARDS HAVING A STRONG RELATIONSHIP TO THIS SAFETY GUIDE

IEC 60960	Functional design criteria for a safety parameter display system for nuclear power stations
IEC 60964	Nuclear power plants – Control rooms - Design
IEC 60965	Nuclear power plants – Control rooms - Supplementary control points for reactor shutdown without access to the main control room
IEC 61227	Nuclear power plants – Control rooms – Operator controls
IEC 61771	Nuclear power plants - Main control-room - Verification and validation of design
IEC 61772	Nuclear power plants – Control rooms – Application of visual display units (VDU)
IEC 61839	Nuclear power plants. Design of control rooms. Functional analysis and assignment
IEC 62241	Nuclear power plants. Main control room. Alarm functions and presentation
IEEE Std 845	IEEE Guide to Evaluation of Human System Performance in Nuclear Power Generating Stations
IEEE Std. 1023	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 Std. 1082	IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations
IEEE Std. 1289	IEEE Guide for the Application of Human Factors Engineering in the Design of Computer Based Monitoring and Control Displays
IEEE Std 1707	IEEE Recommended Practice for the Investigation of Events at Nuclear Facilities”
IEEE Std 1786-2011	IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities

TABLE I–2 RELATIONSHIP BETWEEN INTERNATIONAL STANDARDS, RELEVANT GUIDES AND THE TOPIC AREAS OF THIS GUIDE

This Safety Guide	Internationally Used I&C Standards
1. Introduction	
2. HFE Programme Management	IEC 61513, IEEE 1023, IEEE 1074, IEC 61513, ISO/IEC 15288, NUREG–0711, Human Factors Program Review Model. Rev. 3, INL/CON–12-25117, Towards a Unified HFE Process for the Nuclear Industry. Jacques Hugo, July 2012 ISO/IEC 15288:2008(E); ISO 11064:1-7; IEEE Std 15288–2008, Systems and Software Engineering – System Life Cycle processes
3. Analysis	IEC 61839, IEEE Std 845, IEEE 1082, NUREG–0711, Rev. 3, IEEE Std 1707-2015, IEEE Recommended Practice for the Investigation of Events at Nuclear Facilities, NUREG/CR-6400
4. HFE Design	
– Control rooms	IEC 60964, IEC 61227, IEC 61771, IEC 61772, IEC 61839, IEC 62241, IEEE 576, IEEE Std.1289, NUREG–0700, EPRI – Human Factors Guidance for Control Room Design and Digital Human–System Interface Design and Modification (2004)
– Supplementary control rooms	IEC 60965, NUREG-0700
– Safety Parameter Display Systems	IEC 60960, IEEE 497 (in revision), NUREG 0700, NUREG-0696
– General principles relating to human factors engineering for I&C systems	IEEE 1023, IEEE 1082, IEEE 1289
5. Human Factors Verification and Validation	NUREG-0711, Rev. 3
6. Implementation	IEC 61839, IEEE Std 845, IEEE 1082, NUREG–0711, Rev. 3,
7. Human Performance Monitoring	IEEE Std 845, NUREG–0711, Rev. 3
8. HFE Integration	IEC 61772, IEC 62241, IEEE Std. 1289, NUREG–0711, Rev. 3
– General principles relating to human factors engineering for I&C systems	IEC 61513, IEEE 1023, IEEE 1082, IEEE 1289
– Computerized procedures	IEC 62646, IEEE 1786

REFERENCES TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR 2/1 (Rev. 1), IAEA, Vienna (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 (2016 Edition), IAEA, Vienna (2016): http://www-ns.iaea.org/standards/safety-glossary.asp*

The symbol (*) denotes definition that differs from that provided in the IAEA Safety Glossary.

concept of operation.* A concept of operation 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. Concept of operation describes how the plant is operated (operational philosophy) and includes items such as crew size and makeup how the operating personnel operate the plant under normal and abnormal conditions.

computerized procedure system. System that presents plant procedures in computer–based rather than paper–based format.

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

human-machine interface. The human-machine interface is that part of the system through which personnel interact to perform their functions and tasks. The HMI is constituted by interface between staff 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 that is able to control movement, including strength and fine movements.

human, technology and organization. System as a whole in which the interactions between technical, human and organizational factors are duly considered) are essential to the specification and application of adequate safety measures and the fostering of a strong safety culture.

human, technology and organization system: System where humans, organizational structures, rules and technology interact to fulfil the specific function the system is created for.

important human tasks: tasks that may have adverse or positive effect on operational safety, as determined by safety analysis.

situation awareness. The dynamic process of perception and comprehension of the actual plant's condition in order to support the ability to predict the future systems conditions by the individual and team. A way of forming a mental model of the situation and future planned

actions. The degree of situation awareness corresponds to the difference between understanding of plant conditions and actual conditions at any given time. One of the objectives of HFE is to support the formation of situation awareness of operating personnel.

verification.* Confirmation by examination and by provision of objective evidence that the HMI system meets the design specifications, requirements and provides the support needed to accomplish tasks, as intended.

validation.* Confirmation by examination and by provision of objective evidence to ensure that the HMI system, including the user, can successfully perform that system's intended functions, goals and objectives in the anticipated range of operational environment.

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
Ito, K.	MHI Nuclear Systems and Solution Engineering, Japan
Johansson, Y.	The Swedish Radiation Safety Authority, Sweden
Illobre, F.	Tecnatom, Spain
Laarni, J.	VTT Technical Research Centre, Finland
Ngo, C.	Candesco, Canada
Obenius Mowitz, A.	The 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.	The Swedish Radiation Safety Authority, Sweden
Tasset, D.	Institute for Radiological Protection and Nuclear Safety, France
Yllera, J.	International Atomic Energy Agency