Date: ~~17~~ 2 ~~July~~ November 2017

IAEA SAFETY STANDARDS

for protecting people and the environment

Draft J~~I~~[?]

Step 10

Second internal review of the draft publication

Reviewed in NSOC (Asfaw)

Note:

Resolution to Member States comments can be seen in Draft E, step 9. Several 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 application of ~~the~~ human factors engineering (HFE)[1] [HFE can be defined up front – it might not be quite clear how the term is used in the standards] to meet the requirements established in IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [1], No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [2], and No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities [3].

1.2. This ~~publication~~ Safety Guide takes into account developments, experience and practices in integrating ~~human factors engineering~~HFE into the design of nuclear ~~facilities~~ power plants [?] throughout their lifetime ~~plant lifecycle~~. It references and takes into account other IAEA Safety Standards that are relevant and related~~ing~~ to the integration of HFE in design.[‘HFE design’ is not a very clear expression – in some places you talk about integrating HFE in design, or application of HFE in the design, which is clearer – there can only be one design for any plant] ~~Most notable among these are~~These include the Safety Requirements, IAEA Safety Standards Series No. GSR Part 2, Leadership and Management for Safety, [4], ~~Leadership and Management for Safety,~~ and its supporting Safety Guides IAEA Safety Standards Series No GS-G-3.1, Application of the Management System for Facilities and Activities [5]~~, Application of the Management System for Facilities and Activities,~~ and No. GS-G-3.5, The Management System for Nuclear Installations [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 (HMI), for achieving compliance with the requirements established in SSR-2/1 (Rev. 1) ~~Ref.~~ [1];

— Integrating ~~of~~ HFE into the design of a nuclear ~~facilities~~ power plant throughout ~~the~~ its lifetime, ~~plant lifecycle~~ for achieving compliance with the requirements established in GSR Part 2~~Ref.~~ [4];

— The HFE processes [plural?] to be ~~considered~~ applied in ~~achieving~~ the design of the HMI, ~~human machine interface design across~~ for all plant states;

— ~~The HFE~~Human performance monitoring [HFE performance monitoring not used elsewhere in this Guide] and~~,~~ evaluation and integration of HFE into safety processes, applications and product selection.

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

Formatted: Font: 9 pt

Formatted: Font: 9 pt

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

— Development and review of the safety analysis report;

— Plant modifications and modernizations [modernization has to be a singular word – it is a conceptual approach for a plant/system as a whole – whereas modifications are plural for individual components – you have used it correctly in para 3.3; but SSR-2/2 only mention modifications, so I would prefer to drop 'modernization and modification' as a concept in this guide to the extent possible, as how or whether it differs from 'modification' as it stands in SSR-2/2 is not clear (i.e. is M&M more or the same as just M? if it is more, then what else does it encompass? if it is the same, then why do we need a different term for it?)] for achieving compliance with the requirements established in SSR-2/2 (Rev. 1) Ref. [2];

— Periodic safety review.

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

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

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

— Commercial off the shelf products;

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

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

OBJECTIVES

1.8. The objective of this Safety Guide is to provide a structured approach and guidance on application of HFE in the design and modification of human machine interfacethe HMI 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 necessary to design and validate the HMI human machine interface and to establish [what is the correct verb here? I don't think it can be

'to design and validate the basis'] 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 Safety Guide may [there has recently been a lot of effort made in SGs originating from your section (e.g. DS449, DS482) to clarify the use of 'may'. Assuming that the same applies for DS492, I have retained 'may' only when the meaning of 'giving permission' is intended. Otherwise (i.e. for the other meaning of 'it is possible'), I have changed to 'might' or 'could'] 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. Theis recommendations of this Safety Guide is are meant to be applied using in accordance with the a graded approach, [or the systemic approach? not clear which approach – there are two in GSR part 2] defined as set out in GSR Part 2Ref. [4].

1.12. This Safety Guide applies to implementation application of the HFE aspects of in the HMI design, operation and maintenance of the HMI for new plants designs, as well as for modifications of the HMI of [?] existing plants.

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

1.14. This Safety Guide does not address intentional unauthorized actsthe application of HFE for purposes of nuclear security.[meaning correct?]

STRUCTURE

1.15. Section 2 provides guidance for the management of an HFE programme. Section 3 provides recommendations for HFE analyses review of operating experience, functional requirements analysis and function allocation, tasks analysis, staffing, organization and, qualification, and treatment of important human tasks. Section 4 provides recommendations for application of HFE in design. Section 5 provides guidance on verification and validation of human factors in the design process. Section 6 provides recommendations on the implementation of the design of the HMI design. Section 7 provides recommendations on monitoring human performance aspects of systems performance during the plant operation. Section 8 provides recommendations on the application of HFE in design for computerized procedures, alarm filtering and management[alarm filtering and alarm management are in Section 4, not Section 8]. Section 9 addresses topics related provides recommendations onto the integration of HFE integration in safety processes. Section 10 addresses topics related toprovides recommendations on the application of HFE in the specification and selection of products selection

Formatted: Highlight

Formatted: Font: 11 pt

specification for subcontracted procurements.

1.16. The Annex I provides a list of international industrial standards for instrumentation and control (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."

Formatted: Indent: Left: 0.3 cm

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

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

2.6. An HFE programme should be developed and documented.

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

— Human factors (e.g. knowledge and expertise, cognition, performance expectations, motivation, stress, strength and anthropometrybody sizes);[anthropometry means the study of body sizes]

— Technical factors (e.g. technology, including controls and displays, software, hardware, tools, equipment, plant design and plant processes);

— Organizational factors (e.g. the management system, the organizational structure, governance, resources, staffing levels, and the roles and responsibilities of managers and other plant personnel).

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

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

2.10. The HFE programme should follow be applied using [not clear how a programme can follow an approach? is it its application or its development?] the graded approach, as defined set out in GSR Part 2Ref. [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 [activities? what is HFE processes plural?] as well as the inputs to and outputs for from these processes. The HFE processes [are these not HFE activities?] include analyses, design of human-machine interfacethe HMI, evaluations, such as verification and validation, and monitoring of human performance (see para. 2.19).

2.12. The HFE programme should identify the integration ofspecify how HFE is integrated with other plant design or modification activities.

2.13. The HFE programme should identify the necessary coordination required between personnel responsible for the HFE programme, project and design authorities, and personnel from otherdifferent disciplinesorganizational units in the plant [discipline is not usually used in this way] in order to perform HFE activities.

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

2.15. The HFE programme should identify the responsible organizational requirements [? or the responsible organizational unit?] and competence requirements (e.g. qualifications, skills, knowledge, training) for personnel performing human factors engineeringHFE activities.

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

2.17. The HFE programme should specify that HFE has representation in the design team has a member or members with HFE expertise, as opposed to being remote to the design team.

2.18. For the design of a new plant design, the utility operating organization should assure itself that

the intended plant design ~~has followed~~meets appropriate HFE standards and ~~elements~~ the recommendations of this Safety Guide.

THE HFE PROCESS MODEL

2.19. The overall HFE process can be ~~grouped under~~divided into the following HFE activities: [is there a difference between HFE process and HFE processes, and between HFE activities and HFE processes (plural)? they seem to be used in the same way, to mean those same 6 things (programme management, analysis, design, V&V, implementation, HPM)]

— Programme management;

— Analysis;

— Design;

— Verification and validation;

— ~~Design i~~Implementation of the design;

— Human performance monitoring.

HFE ACTIVITIES WITHIN AN ENGINEERING ~~PHASES~~PROJECT

2.20. ~~Interactions of~~ HFE activities should be integrated into the basic ~~phases~~ stages of an engineering ~~process~~project [?],[you talk about engineering processes, engineering phases, and engineering projects at various points below, and the difference is not clear – an engineering project seems to work well] as illustrated ~~by the example provided~~ in Fig. 1.

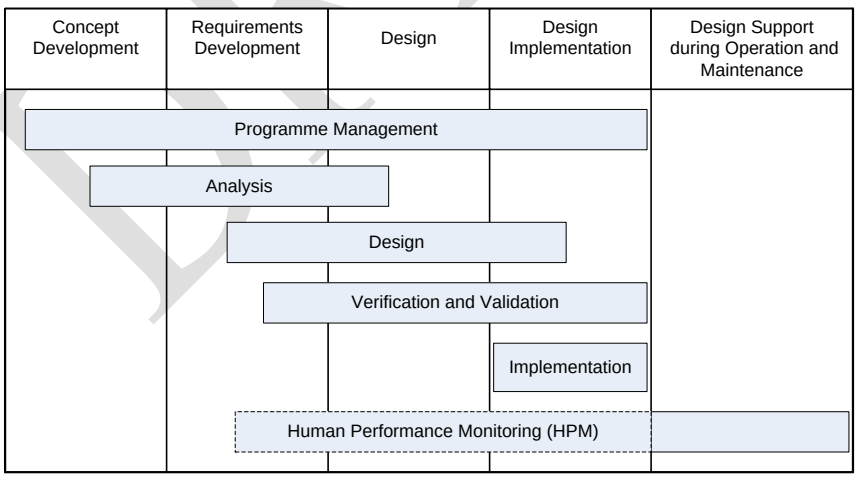

FIG. 1. An example of a ~~HFE~~ generic engineering ~~process~~project [?], indicating when HFE activities are undertaken.

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

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

— HFE programme management [?] should establish a capable human factors organizsational unit with responsibility for human factors and with sufficient authority on at all hierarchy -levels to effect the 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 engineering project;

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

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

— HFE analyses should help be used to identifying the organizational architecture structure that frames the use of the HFE systemprogramme [? this is the only time HFE system is used; or maybe HFE process?], i.e. the identification of users, their roles and responsibilities, required qualifications and, regulatory requirements, and which supports the developing concepts of [what is developing concepts of operation and maintenance?] operation and maintenance;

— HFE analyses should provide a preliminary understanding of the allocation of functions allocation, and the human information requirements for monitoring and controlling (where applicable) the functions of a systems in the plant;.

— HFE analyses should provide insights and consideration of how operators should are expected to respond in the presence of control system failures and HMI failures. [I turned this from a stand alone para into a bullet in the list]

Formatted: Style2, No bullets or numbering

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

— Results of the function analysis that identify the functional requirements for the systems, structures and components [what is 'the system'? or could we just wait to Section 3 to define 'function analysis' more precisely];

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

— Results of task analyses that provide insight into:

a) The Ppossible sequence and flow [what is flow if not sequence?] of tasks;

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

c) Safety significant complex tasks that warrant detailed analyses technical and HFE evaluationanalyses;[what is the difference between HFE analysis (used a lot in this Safety Guide) and HFE evaluation (used rarely)]

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 necessary to support the task.

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

2.23. The following HFE inputs should be considered as HFE inputs forin the design phasestage:

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

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

— Specific HFE design principles and HMI design [?] guidelines for maintenance and testing considerations;

— The Ppotential impact of new or modified designs to on human performance, procedure the development of procedures and training;

— Collection and analysis of user feedback through early HFE evaluations analyses in the form of prototype or concept usability testing and user reviews of prototypes and concepts;[OK? pls check which adjectives apply to which nouns in this bullet]

— 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 tobe considered [as in previous paras?] as HFE inputs for the design implementation phasestage:

— 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 haves been provided in the design;

— HFE Vvalidation in respect of human factors to ascertain [elsewhere you rarely talk about HFE validation] of the degree to which the HMI design and supporting mechanisms facilitate the achievement of safe operation of the plant;

— Confirmation of the feasibility of important human tasks identified as important to safety[pls check – a task is not usually 'important to safety' - this is an attribute of an item] in the probabilistic and deterministic safety analyses through HFE validation in respect of human factors;

— Confirmation of the completion of HFE analyses and of HFE inputs into the design in accordance with HFE planning [this is the only place you refer to HFE planning] of the HFE programme and regulatory expectations.

2.25. Throughout the design stages, consideration should be made ofgiven to the constraints of the technology being considered, e.g. availability, reliability, band-width, and general acceptance and familiarity of personnel with the technology. For example, although personnel accept the use of digital technology in everyday life,; [do these two phrases link together? or are they to be separated by an 'or'?] the designer may wish need to consider whether the use of virtual reality or augmented reality has the potential to would cause issues difficulties for personnel.

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

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

2.28. HFE activities that 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 organizational units participating in the design.

2.29. The HMI and its functionality should be treated from the perspective of the HMI being part of an integrated whole and not merely 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 Ddata and conclusions from event analyses should be used as an HFE inputs for the design of the a new plant or the modification of operating an existing 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 difficulties in current designs that may might be addressed met [or "might need to be addressed"?] during plant modernization and modifications to plant components; and (c) to evaluate relevant industry experience with design options to for instrumentation and controlI&C systems and HMI technology for their potential to improve plant efficiency and safety.

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

3.5. The review of operating experience review should [?] providestake into account ['provide' implies it's an output, while this seems more like an input, or the scope] the following:

— Applicable HFE related issues identified in the review of plant operating experience at the nuclear power plant;

— Issues identified from in the review of applicable predecessor designs;[or identified at nuclear power plants with earlier designs? how does this differ from the last bullet?]

— Experience insights identified by plant personnel;

— Issues identified in the review of Ooperating experience from at other nuclear power plants and in other industries.

3.6. HFE should consider Ooperating experience data for any of the following should be taken into account:

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

— Adverse Ttrends that that could indicate a reduction indetract from reliability;[how do trends detract from reliability?]

— Existence of Data on root causes data that could point to a need for [?] improvements in design;

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

— Corrective actions identification and their implementation;

— Recurring events;

— Reviews of maintenance practices;

— Industry ~~notices~~ communications on best practices.

3.7. IAEA Safety Standards Series No. SSG-50, Operating Experience Feedback for Nuclear Installations ~~Ref.~~ [7] provides recommendations for establishing, implementing, assessing and continuously improving an operating experience programme for nuclear installations to prevent or minimize the risk of future events by learning from events that have already occurred at the installation or elsewhere.~~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~~. [I updated this sentence to the main objective of DS479, which will be published before DS492]

FUNCTION ANALYSIS

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

~~3.9.~~3.8. A ~~F~~function analysis should be conducted for all plant states to ensure that the functions necessary to accomplish safe operation of the nuclear power plant are sufficiently well defined and properly analysed. [we need to put the definition of function analysis up front in this section, it is not used in other standards]

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

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

3.11. The f~~F~~unction analysis should ~~also~~ provide time and performance requirements and constraints for performing the functions.

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

3.13. The f~~F~~unction analysis should ~~help~~ be used to identify~~ing~~ high level acceptance criteria associated with maintaining safe operation of the plant.

3.14. As part of the function analysis ~~process~~,[function analysis process not mentioned elsewhere] the following should be analysed and documented:

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

Formatted: No bullets or numbering

Formatted: Indent: Left: 0 cm

— Relationships ~~between high level functions and the plant's systems~~ (e.g. the plant configurations or 'success paths'[2][success paths is not clear; footnote below adapted from text in NS-G-2.13, but maybe not correct here]) between high level functions and the plant's systems responsible for performing thosee functions; [this bullet is not clear – does the bracket contain examples of the relationships or examples of the systems?]

— ~~Higher level functions should be~~The decompositioned of high level functions into lower level functions that can be mapped to tasks to be performed by plant automation or by~~the~~ humans, or by humans 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 actions required for the success path should be documented as part of the function analysis.

3.16. ~~The function analysis should document~~ Ddependencies that ~~may~~ might exist among plant functions, systems and their support systems should be documented as part of the function analysis.

FUNCTION ALLOCATION

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

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

3.19. Human, technology and organizational 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 f~~Functions allocation makes use of the function analysis [OK, as in previous subsection?] of plant control ~~functions~~ systems and ~~lays out~~establishes the allocation of control processes, which ~~may~~ might [or should?] be assigned in the following ways:

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

Formatted: Font: 9 pt

Formatted: Font: 9 pt

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

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

— To aA combination of personnel and automation, for example:

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

3.22. In addition to consideration of human capabilities, when allocating functions, the designers should also include take into account such factors as whether the technology readinessis well established [or do you mean whether the technology is acceptable to personnel?], timinge requirements capabilities [or timing requirements associated with the function?] associated with systems response, and considerations for defence in depth.

3.23. If the achievement of a control function requires the allocation ofing overlapping and redundant responsibilities to personnel and to automation (e.g. assigning personnel the responsibility of monitoring and maintaining supervisory control over automaticed [this is the usage elsewhere in the text] systems), this allocation should be documented.

3.24. The nature and scope of human tasks across functions should be documented for all functions.[across functions is not clear]

3.25. The Aallocation of functions should be analysed for all [all? or just selected (different)?] different operational states and accident scenariosconditions.

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

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

TASK ANALYSIS

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

3.29. Human, technology and organizational factors (e.g. leadership, management and

communication) should be considered when performing conducting the task analysies.

3.30. Task analysis should be conducted to analyse and document the 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 the user in order towho will accomplish the task.

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

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

— Tasks which that vary differ depending on the plant statewith the operational and accident scenarios;

— Tasks which that require individual work and/or co-operation/ or exchanges between different disciplines organizational units (e.g. operations, maintenance, procedures development, computer systems engineering) and interested parties;

— Tasks which that must sometimes have to be performed under time pressure or, harsh environmental conditions and contexts, or that are extremely vitalsafety critical [‘extremely vital’ is not a phrase used elsewhere in the standards, but you do talk about safety critical tasks elsewhere in this Guide] and rarely performed.

3.33. When identifying the tasks, the following considerations to the rRisk and safety aspects should also be considered when identifying the tasks to be included in the task analysis, which may could include:

— Tasks with posing an occupational risk to the personnel;

— Tasks credited in the safety analysis report;

— Tasks identified from operating experience 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 that are critical for maintaining the plant in a safe state or restoring it to this a safe state following an event.

3.34. Responses to alarms, and surveillances, [what is response to surveillance? or is it surveillance tasks?] and maintenance tasks directed from the control room by operators should also be analysed.

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

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

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

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

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

— The ~~order~~ sequence for implementing tasks and subtasks;

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

— The ~~human~~ [the performance requirements are for the task, right? (not for the humans)] performance requirements and constraints (e.g. time, precision and~~,~~ independent verification);

— Required communication systems and access to those systems.

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

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

— Knowledgeable personnel from the design team, operating personnel who have gained operating experience in similar plants, ~~stakeholders~~ interested parties [who are these likely to be?] and experts [who are these likely to be, if not already listed?];

— Walk~~-~~through and talk~~-~~through to analyse ~~the~~ tasks performed by a predecessor system~~'s task activities~~ and tasks from similar plants, as well as the tasks ~~related to~~associated with the system being developed;

— Data from the review of operating experience ~~review~~ (~~e.g. note~~ with account taken of [what does 'note' mean? how does it relate to 'e.g.'?] differences from the reference design);

— Data from the customer's requirements;

— Data from other analyses that are inputs to the HFE design process (e.g. function~~al requirements~~ analysis, function ~~and~~ allocation, human reliability analysis and training needs analysis);[merged with next bullet – I think they were the same]

~~— 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 the 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 for the task on human reliability should be evaluated.

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

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

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

3.42. The results of the task analysis can be directly used to support the human error reliability analysisassessment. [human error assessment not mentioned elsewhere]

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

3.44. A Ttable top analysis of documentation (e.g. procedures) alone may might not be sufficient for determining that whether a task(s) can be performed. Stakeholder Iinput from interested parties [who will these probably be?] and/or simulations supported by mockups, field plant [?] walkdowns, partial task simulators, or full scope simulators may be performed to confirm the feasibility of the actions tasks in real scenarios.

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

Formatted: Highlight

STAFFING, ORGANIZATION AND QUALIFICATION

3.46. Staffing, the organizational structure [OK?] and the qualifications of personnel should be analysed for their impacts on important human tasks important to safety [or safety critical tasks?] to determinethat the required number of personnel, organizational interactions and qualifications of personnel are sufficient for task performance.

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

— The safe completion of humanthe operator tasks;

— The workload of the members of a teampersonnel;

— The ability to synchronize align the contribution of each team member to with the a team's task;

— The independence and coordination cooperation of the individuals responsible for checking the progress of tasks [checking what? or do you mean HPM?] (for example, checking actions taken in the control room and locally by the operators);

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

3.48. Staffing, organization and qualification analysis should cover all the working groupsteams [pls check – you use team, work group and working group – I think they all have the same meaning] that carry out tasks with an safety impact on safety (see paras 3.28 to 3.45 on task analysis). This includes all teams of operating personnel, service support teams and, emergency preparedness and response teams. The analysis should identify and evaluate the needs of these working groupsteams in terms of staffing, organization and qualification.

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

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

— Concept of operations in normal operational states and accident conditions;

— Design requirements;

— Task requirements;

— Regulatory requirements;

— Operating experience;

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

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

3.52. The following should be considered when assigning individual tasks to work groupteam 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 states and accident scenariosconditions;

— The impact on human performance impact is assessed taken into account when distributing the tasks between teams working during the day and working at night;

— The tasks required in various operating situations are assigned to work groupteam members in a manner that order to ensures continuity of responsibilities and maintaining individual and collective team [used elsewhere and also in definition] 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 iImportant 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 both operational states including and responses during in accident conditions.

3.56. An analysis supporting the application of HFE in design for safety ['design for safety' is not used elsewhere] 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 factors that impact performance shaping factors, should be analysed, and the ability forit should be confirmed that the design solution to achieve the necessaryis such that human performance related to safety requirements relating to human performance will be met should be confirmed.

3.58. Regardless Irrespective of which the underlying approach is taken to identifying important human tasks, the HFE design [surely the whole design? not just the HFE design], procedures, training, staffing levels, and concept of operations should support the execution of important human decisions and actions.

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

4. APPLICATION OF HFE IN DESIGN

GENERAL HFE GUIDELINES

4.1. Requirement 32 of Ref. SSR-2/1 (Rev. 1) [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 SSR-2/1 (Rev. 1) Ref. [1] states that:

> "The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall 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 SSR-2/1 (Rev. 1) 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 decisions to act shall be simply and unambiguously presented."

4.4. The HMIhuman machine interaction [or do you mean something more general like "the means for interaction between humans and machines"?]should be designed through a structured methodology that permits, from conceptual design, the identification and selection of candidate HMI approaches, the definition of a detailed design, and the performance of HMI tests and evaluations, when necessaryneeded.

4.5. The concept of defence in depth should be considered applied duringin the design of the 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 apply athe human-centred approach in which considers the equipment and systems are considered from the perspectives of the personnel who would will carry out the associated functions and tasks associated with the design.

4.7. The hHuman aspects, the machine technology (both hardware and software), the working environment, and the control, operational and management strategies [it is strategies in the para 4.9] to be applied should be considered taken into account during at all phases stages of the design process (in accordance with an integrated, systemic approach).

4.8. The Ddesigners should consider how information relayed by the HMI will be communicated,

exchanged and used by different groups (e.g. staff in the main control room and in, emergency response facilities).

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

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

— Whether automatic actions are properly allocated to respondfor response to a postulated initiating event;

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

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

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

— Whether utility implementation by the operating organization of 'stress tests' for of the response of plant systems in a presence ofto severe accidents may provides insights for how operators and responders [not clear what a responder is in this situation (usually used in the EPR area in the context of a 'first responder' (see Glossary); term is not used elsewhere in this SG] may might be able to use equipment differently for purposes different from the original intent in order to possibly achieve safety functions;

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

— Whether equipment could be used out of its design function intent to support, the adoption of a different strategy (e.g. use of the 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 at 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 availability of sensor data availability);

— The Pphysical environment in which the HMI is to be deployed;

— Cognitive limitations and strengths of the users;

— The Kknowledge, skills and abilities of personnel, including personnel from various user/occupational typesgroups;

— Applicable regulatory requirements.

4.13. The HMI design should support the roles of plant operators in the plant, considering and should take into account 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 necessary needed to control the plant during a range of operating conditionsplant states, from normal operation through to accident conditions;

— Detailed information and control [or "I&C"?] requirements (e.g. requirements for display range, precision, accuracy, and units of measurement);

— Requirements relating to aspects that Task support requirements tasks, including habitability (e.g. lighting and ventilation requirements).

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

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

4.17. This documentation guidance [same as previous sentence?] should define specify the detailed design criteria for the HMI elements. In case ofIf the HMI modernizations in an existing plant undergoes modernization, it the guidance should be evaluated for any necessary needed revisions based on both the HMI modernization needs and the concept of operations.

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

HMI Detailed design of the HMI and its integration in the overall design of the plant [integration in what?]

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 conditionslevels, flooding, steam ingress and limited ventilation.

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

4.22. The presentation of Iinformation should be integrated [you would need to say integrated with what] presented in a manner that optimizes the understanding of operators of the status of the plant and the activities necessary to control the plant.

4.23. The operation and appearance of the HMI should be consistent across information and control [or "I&C"?] locations and platforms[platform not used elsewhere; doesn't location cover it?].

4.24. To the extent possible, the HMI should be designed to prevent and detect operator errors, in particular [?] in cases where an action might be taken in an incorrect context, or with an inappropriate plant configuration. This includes design to ensure the 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 might be presented.

4.26. To the extent possible, information flow diagrams and control performance actions [what is control performance? not elsewhere in text] should complement the information processing capabilities and the performance of operators.

4.27. The design of the HMIhuman 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 crewstaff, e.g. via by means of 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 digital [normally "analogue and digital" go together; or maybe you mean "audio and video"?] video displays without significant interruption of control actions;

h) Should reflect consideration of human cognition, physiological characteristics, characteristics of human motor control and anthropometryhuman body sizes.

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, [OK to delete comma?] procedures and the training programme should be designed and compared to ensure consistency with each other.

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

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

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

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

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

— Consistently To be consistent as far as possible with users' existing strategies for gathering and processing information and executing actions identified in the task analysis.

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

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

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

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

4.38. The HMI design should determine take into account [OK? not clear how the design can

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

HMI tTests and evaluations of the HMI

4.39. Usability tests of concepts and detailed design features should be conducted during the process of developing the 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 on [?] other design considerations. These Such trade-off evaluations should consider:

— Personnel task rRequirements for [important?] human tasks;

— Human performance capabilities and limitations;

— HMI system pPerformance requirements for the HMI;

— Inspection and testing needs;

— Maintenance demands;

— The Uuse of proven technology and the operating experience of predecessor designs.

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

Design guidelines for of the HMI controls

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

4.43. HMI controls may be implemented as 'soft' controls (see paras 4.50 to 4.61), as multiplexed, or dedicated, control devices, and or as a combinations thereof. [this sentence needs some work to show how the list breaks up, and to explain all these terms, which are appearing for the first time or the only time; maybe a footnote or two?]

4.44. Analogue control devices (e.g. push buttons, rotarydials [what is a rotary?], slides, toggle switchess and, rocker switches) are suitable for controls that are in constant use, for example an electrical output, or and those for controls whose immediate accessibility and reliability are of prime importance, for example an emergency trip button.

4.45. Controls should provide optical and/or acoustical [used elsewhere – better to be consistent one way or another] visual or auditory feedback within an adequate time to indicate that the system has received a control input.

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

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

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

— Locating controls at proper positions;

— The use of protective structures;

— A demand for [?]

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

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

4.49. To minimize operator errors, control movements should conform to characteristics relating to the reach, vision and comfort of operators [pls check, I took this phrase from para 4.62 – stereotype is a negative word in English – or perhaps you mean they should *not* conform to stereotypes?] (e.g. it should meet users' expectation) and should be compatible with the attributes of the controlled variable.

Formatted: Font: Italic

Design considerations for soft controls

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

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

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

4.53. Soft controls should provide display devices:

— To allow access to individual components when necessary;

— To allow access to information about the status of each component;

— To control the relationship to other components.

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

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

4.56. Input formats commonly used with soft controls systems are discrete adjustment control interfaces[OK? google likes this term more than the original], soft sliders and arrow buttons. Input formats for entering data should be provided in the soft controls.

4.57. The cCursors should have a distinctive appearance; and their movement should have a sensitivity compatibility with the required tasks and operators' skills. Their movement should conform to characteristics relating to the reach, vision and comfort of 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 the options and controls that are available for selection. The options should be listed in a menu added to the working display without requiring the operator to remember memorize them or to access a separate menu display.

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

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

Application of HFE in the design for of workstations

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

— Workstation height;

— Inclination of Bbenchboards slope, angle, and depth for of consoles and sit stand workstations that can be adjusted for sitting and standing;

— Control device location;

— Display device location;

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

— Size and legibility of text and graphics for legibility;

— Clearance spaces 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 and other operators.

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

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

4.66. Functions and process operations should be grouped into Ffunctional groups should be specified in terms of the achievement of a given in accordance with their characteristics function or process operation.

4.67. Types of grouping that may be used for building fFunctional groups should be organized by function, by sequence of use, by frequency of use, by priority, by operating procedures or by a system with mimic display arrangement[3] [could you put a footnote explaining what a mimic display is? – it might not be commonly known].

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

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

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

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

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

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

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

Formatted: Font: 9 pt

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

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

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

— Contingency space for special test equipment or for access for [?] repairs.

APPLICATION OF HFE IN DESIGN FOR ACCESSIBILITY AND THE WORKING ENVIRONMENT

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

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

4.76. Paragraph 5.61 of SSR-2/1 (Rev. 1) 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 in which operating personnel are expected to monitor and control plant systems, the necessary provisions should be made to ensure suitable conditions in the working environment and to protect against hazardous conditions.

4.78. Normal [I deleted 'normal' so as not to confuse with normal operation] aAspects of the working environment to that should [a should statement?] be considered include lighting, temperature, humidity, noise and vibration.

4.79. Hazards to that should 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 routes that should beare protected against potential internal hazards or and external hazards to supplementary control points and other field locations where operator actions are expected to occurbe taken.

MAIN CONTROL ROOM

4.81. Requirement 65 of SSR-2/1 (Rev. 1) 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 SSR-2/1 (Rev. 1) 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 SSR-2/1 (Rev. 1) 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. TheA control room design should be consistent with the concept of operations, which should describes how the plant will be operated in all plant states.

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

— Operational Operating goals and objectives, including safe operations;

— The Oorganization of the HMIs into workstations (e.g. consoles and panels);

— The Aarrangement of workstations and supporting equipment in the main control room.

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

— Recognize the actions being taken by the reactor protection system and other automatic systems;

— Analyse the cause of disturbances and follow their course;

— Perform any necessary manual counteractions.

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

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

4.90. The display system should communicate the intended information to the operator without ambiguity or loss of meaning, or [all systems have a latency, right? so we need to apply 'unnecessary' to that attribute too] unnecessary time delay or latency.

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

4.92. Numerical values should be displayed only to the level of significance required of the data for operation, regardless irrespective of higher levels of significance of individual input data.

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

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

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

4.96. Information from the HMI information should allow operators to immediately assess the overall plant status and detect conditions that require attention without performing the need for interaction with the HMIinterface management tasks.[OK?'interface management tasks' not used elsewhere]

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 overload of the display system overload or other system conditions may could result in a processing delay, the system should acknowledge the data entry and, should provide the operators with an indication of the delay and of [OK?]the completion of the processing to the operator.

4.101. The HMI for real time tasks requiring fast response by operators response should require only

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

4.102. User assistance should be provided by the video display unit systems. It Such assistance should [OK to write 'should'?] 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 ofentering commands entry (e.g. the required syntax, parameters and options).

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

4.105. A standardThe display screen organization should be evident organized such thatfor the location of various HMI functions (such as a the data display zone, the control zone and the or message zone) is standardized from one display to another.

4.106. The HMI display system should clearly indicate which items are selectableavailable for selection. [same as para. 4.59?] When the operator is performing an operation on some selected display item, this item should be highlighted in order to avoid errors.

4.107. The HMI should be user friendly, without requiring and should not require the operator to memorize special additional and or varying codes or sequences to perform translations and conversionsactions [translations and conversions not mentioned elsewhere].[same as para 4.60?]

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

Layout of the Mmain 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.[what does this mean? could it be deleted?]

4.110. Main control room staffing and task assignments should ensure be such complete and timely coverage ofthat controls, displays, and other necessary equipment required are accessible [not sure what complete and timely coverage means?] completely and in a timely manner forduring all modes of operation.

4.111. The Llayout of desks workstations [desks not mentioned elsewhere] and consoles in the main control room:

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

— Should facilitate ~~voice~~ verbal [you use verbal communication elsewhere, and I think you mean the same thing] communications from operators at the workstations to any point in the main operating area;

— Should permit access to workstations without ~~having~~ the need to overcome obstacles;

— Should permit efficient, unobstructed movement and communication.

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

4.113. A storage space ~~of~~ for emergency equipment that control room ~~personnel~~ staff ~~may~~ might require during an accident ~~conditions~~ should be provided, with ease of access to the space.

Habitability considerations

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

4.115. ~~Workspace~~ The design of the workspaces in the main control room should consider environmental factors that can have an important effect on personnel performance, including designing for thermal comfort, adequate illumination including in the event of an emergency ~~scenarios~~, auditory environments that promote clear verbal communication~~s~~, and ~~facility~~ suitable layout of the workspaces [what is facility layout in this context? ‘plant layout’?].

4.116. The control room should contain sufficient facilities and supplies to ensure comfortable ~~sustained~~ long term ~~occupancy~~ occupation during a response to ~~design extension conditions~~an accident.

4.117. The control room design should include assessment of and protection against missiles originating from outside the control room. Guidance on ~~the~~ protection of the control room from missiles is provided in ~~Ref.~~NS-G-1.11 [8].

Design ~~guidelines for~~of ~~the HMI of~~ the safety parameter display system

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

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

4.120. The safety parameter display system SPDS should provide information on the critical safety functions associated with the reactorplant design[OK?].

4.121. The safety parameter display system SPDS should be located conveniently for the main control room personnel staff and should provide continuous display information from which the plant safety status [safety status not well defined] can be readily and reliably assessed.

4.122. The safety parameter display system 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 need to survey all information on display in the main control room.

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

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

4.125. The safety parameter display system 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 SSR-2/1 (Rev. 1) 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, with particularly for consideration given to the need to take immediate actions.

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

4.130. Workspace The design of the workspaces in the supplementary control room should consider

environmental factors that can have an important effect on personnel performance, including designing for thermal comfort, adequate illumination including in the event of an emergency scenarios, auditory environments that ensure promote clear verbal communications, and facility suitable layout of the workspaces [what is facility layout in this context?].

4.131. Computer based information or controls used at in the supplementary control room should function in a manner that is 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 for 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 should be established for the transfer of command, controls and communications from the main control room to the supplementary control room should be provided.

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

EMERGENCY RESPONSE FACILITIES ON THE SITE

4.135. HFE should be applied when designingin the design of emergency response facilities[4] including site technical support centres on the site. The design should provide for optimal layout of individual workplaces, and the data and information necessary 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 Factors to be considered include illumination, size, geometry, display and control layouts, availabilitye of content, suitabilitye of format and standardization of the displays., and fFundamentally consideration should be given to 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] 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.

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

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

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

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

4.142. The technical support centre staff should be trained on in the identification and use of the instruments to support the executionimplementation of severe accident management guidelines. More detailed recommendations for the development and implementation of severe accident management guidelines are provided in Ref.NS-G-2.15 [10].

ALARM MANAGEMENT

4.143. Paragraph 5.66 of SSR-2/1 (Rev. 1) 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 deviations 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 included to as status information.

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

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

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

Alarm generation

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

— Digital signals;

— Analogue signals;

— Calculated, [comma?] synthesized or grouped signals from direct inputs or derived from other systems.

4.151. Alarms based on analogue and digital signals should be configurable. The aAlarmed 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 that is consistent with the structured architecture of the plant.[what is the structured architecture of the plant? needs some explanation]

4.153. Alarms generation should be context-aware (e.g. pump low flow alarms should be 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 unnecessary unneeded momentary, or chattering, alarms.

4.155. Alarm systems should be able to reduce automatically the number of alarms being generated at any one time conditions at the signal level.[alarm conditions at the signal level is very unclear; has this got to do with alarm inhibition or alarm suppression or alarm overload?]

4.156. Alarm inhibition takes inactive alarms out of service by disabling alarm generation, normally during testing, maintenance or repair of the associated equipment.[merge paras, and put the sentence

explaining alarm inhibition first]

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

Formatted: No bullets or numbering

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

4.158.4.157. HFE analysis and validation should be used to determine whether one alarm is masking the occurrence of another alarm(s).

4.159.4.158. Alarm systems should support the prioritization of alarms prioritization to determine the relative importance between alarms.

Alarm processing

4.160.4.159. The alarm system should support user-defined generation of alarms 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.

4.161.4.160. Alarm systems should be able to apply event-based and significance-based fundamental[not clear whether the fundamental applies to the alarms or the techniques – maybe it's not necessary?] alarm suppression techniques, as follows, at different hierarchy levels:

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

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

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

Alarm annunciation and control

4.163.4.162. The alarm system should provide visual indications when any alarm condition appears or clears. Visual indications may could include the following:

— 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 sub alarm has already occurred and has been acknowledged.;

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

4.164.4.163. The alarm system should provide auditory indications when any alarm condition appears

or clears.

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

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

Alarm presentation

4.167.4.166. The 'dark-board criterion' consists of minimizing the number of alarms presented during normal ~~operating conditions~~operation without challenging plant safety.

4.168.4.167. Alarm processing should follow the dark-board criterion at full power and ~~recommended~~ [do you mean to say that recommended is less than 'should'? can it be deleted or reworded?] ~~at~~ for other conditions of normal ~~operating conditions~~operation.

4.169.4.168. Alarm presentation should be based on following different types of displays~~s~~:

— Spatially dedicated continuously visible displays (e.g. analogue tile panels or arrays of visual display units with continuously visible tile-like panels, and, 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~~ and soft control displays);

— Individual alarm information displays;

— Mixed displays, ~~resulting from the~~i.e. a combination of the other types of displays.

4.170.4.169. Information about alarm state changes and new alarms [pls clarify] should be presented and managed separately.

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

4.172.4.171. Alarm messages should contain all the information the operators need to respond to the alarms~~m~~ effectively, such as alarm sources, priorities, descriptions, setpoints and parameter values, and references to alarm response procedures and associated displays.

4.173.4.172. Operators should be able to sort alarm messages on demand. The alarm system ~~may~~ could [should?] provide lists of alarms organized by:

— Chronological order;

— Priority levels;

— Alarm state~~us~~;[used elsewhere]

— Tag identity;[what is this? 'tag' not used elsewhere – maybe a footnote to explain?]

— Any other logical order.

4.174.4.173. 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.

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

— Trends for variables from which the alarm is derived;

— Statistics, such as how often on average the alarm has occurred;

— Relationships with other alarms or variables;

— Current or historical work orders or reports relatinged to the alarm.

Alarm response procedures

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

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

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

— The exact message associated with [provided by?] the alarm message;

— Alarm Ppriorities for response to alarms;

— Automatic actions,[the automatic ones would not be operator actions, right?] and immediate and other operator actions;

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

— References.

PROCEDURE DEVELOPMENT OF PROCEDURES

4.178.4.177. Guidance in thisThis section provides recommendations on human factors aspects of procedure development and should be read in conjunction with the recommendations provided in support of Ref.IAEA Safety Standards Series No. NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants [11][10].

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

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

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

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

~~4.181.~~4.180. Procedures should be validated to ensure that they can be executed as specified and that the results or outputs are as intended.

~~4.182.~~4.181. The development of ~~P~~procedures ~~development~~ should also consider inputs from task analyses ~~to~~for the following purposes:

— To ~~I~~identify potential errors that ~~should~~ need to be highlighted in the procedure;

— To ~~P~~provide ~~required~~ the flow of information, actions~~,~~ and feedback necessary for the successful completion of a task;

— To ~~I~~identify links between tasks and personnel;

— To ~~P~~provide preliminary information on the timing of individual actions within the procedure [?] ~~information~~;

— To facilitate the ~~T~~transition between procedures;

— To establish the ~~F~~format and content of technical warnings, pre-requisites (initiating conditions) and requirements for termination of the procedure ~~termination~~.

~~4.183.~~4.182. The expected outcome of an action (or suite of actions) identified in a procedure should be clear, understandable and verifiable.

~~4.184.~~4.183. ~~HFE design input to~~ In applying HFE to the development of plant procedures ~~should consider~~the format and content ~~that is commensurate~~associated ~~of~~ with the category of procedure (e.g. emergency operating procedures, maintenance procedures and test procedures) should be taken into account.

~~4.185.~~4.184. Procedures for ~~S~~safety critical tasks, complex tasks~~,~~ and rarely performed tasks should be set out in a detailed and step-by-~~-~~step manner.

~~4.186.~~4.185. ~~The~~ Each procedure should provide guidance for safe ~~contingent~~ alternative [?] actions if the actions specified cannot be achieved or guidance for terminating the procedure safely.

DEVELOPMENT OF TRAINING PROGRAMMES ~~DEVELOPMENT~~

~~4.187.~~4.186. 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.~~4.187. Operating personnel should be trained on the relationship between the display form and the plant states it is intended to represent, including failure modes and their effect and appearance on

the display representation.

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

4.190.4.189. The training plan should be reviewed and modified periodically according to in accordance with the evolutions of HFE the design.

4.191.4.190. Training should be timely, and training associated with modifications or modernizations, of HFE design to the plant should be completed prior to operationthe modifications being put into effect [meaning correct?].

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

5. HUMAN FACTORS VERIFICATION AND VALIDATION IN RESPECT OF HUMAN FACTORS

GENERAL

5.1. The human factors vVerification and validation of the HMI system in respect of human factors should comprehensively determine that whether 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 and, 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 in respect ofthe human, technical and organizational aspects and their interactions are combined.

5.5. Verification objectives activities [these don't seem like objectives] typically include:

— Identification of HFE standards and guidelines;

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

— Review of design requirements, drawings and, manuals;

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

5.6. Verification activities may might include involve interactions with system users. Validation activities necessarily include are required to be undertaken by user representativesexperts who are independent from of the design team [1]. [pls check meaning – see para 6.37(a) of SSR-2/1 – same concept here or is something else intended?]

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

— The ability of the crew personnel [operators? system users?] 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 ascapability of the HMI to it supports operator tasks;

— The suitability of the layout of the work spaceworkspace to support task and system performance;

— The resources for crisis management and coordination among the team members involved in the management of an accident, including external organizations.

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

— The layout for of the main and supplementary control rooms as it supports the operators[2] tasks;

— The effectiveness of measures relating tothe systems for monitoring, control and maintenance (inside and outside the control rooms);

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

5.9. A vValidation of the integrated system of comprising 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 have already been implemented beforehand, in particular:

— The operating conceptconcept of operations [?] in all operational states and accident conditions;

— The technical and user requirements of associated with the tasks, especially that are safety sensitivecritical tasks [? you used this elsewhere; or do you mean that the requirements would be safety ‘sensitive’?];

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

— Inputs from functional analysis;

— The rRegulatory requirements;

— Inputs from operational operating experience feedback;

— Important Hhuman tasks that are important for safety;

— Data from safety analysis;

— Data from human reliability analysis;

— Data on staffing, organization, and qualifications;

— Data from previous HFEhuman factors engineering reviews and analyses;

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

PLANNING FOR VERIFICATION AND VALIDATION PLANNING

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

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

— As mMore interfaces become available;

— As Pprocedures are become more detailed;

— As Ooperators are trained;

— As Ssimulations fidelity becomes more realistic.

5.13. The verification and validation plannning should specify:

— The Sscope of the evaluation;

— The necessary [?] Ddata collection and analysis;

— Measures of effectiveness;

— Evaluation and acceptance criteria;

— Participants involved in the evaluation;

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

— The test environment;

— The schedule.

5.14. In addition, the validation plan [OK? a separate validation plan? or 'the verification and validation plan'?] should also specify:

— The selection of scenarios;

— Participants (i.e. user selection) and their training;[this is already in the previous para – delete, or explain how it differs from above]

— Materials[5] and tools to be used by the evaluation team.

5.15. The verification and validation plan should also describe the objective and the expected output [probably only output, right? or how will input demonstrate compliance?] that will demonstrate the compliance of the HMI design:

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

— With the plant's operational acceptance criteria;

— With regulatory requirements for operator response.

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

— The analysis and assessment of any HFE related issues;

— The tracking of HFE related issues;

— The approach for resolving design deficiencies.

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

5.18. The participants conducting validation tests should be organized in accordance with the organizational structure [?layout seems like physical layout] for future operation of the plant [?].

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

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

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

TEST METHODS

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

— Static testing (e.g. to verify that the system meets the design specifications);

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

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

— Observation;

— Self-report assessments [OK?self report not a common term] (e.g. questionnaires, and structured interviews[how can an interview be a self report/assessment?]);

— HFE cCheck lists (e.g. within static or dynamic testing);

— Walkthroughs of tasks.

5.22. The test participants should be familiar with the relevant portions of the modificationssystem [? 'portions of the modifications' not introduced till now – isn't the testing just of a system?] before conducting the testhand.

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

PERFORMANCE MEASURES

5.24. HFE Vverification and validation in respect of human factors should apply relevant human performance measures for the actual working environment. These Such measuressments may could include the following:

— The Ccomplexity of task to be performed;

— The Wworkload (e.g. individual and team);

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

— Sequencing and response times;

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

— Requirements for using procedures usage;

— Requirements for detecting and responding to adverse conditions;

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

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

— Time;

— Accuracy;

— Communication frequency and content;

— Error detection and error recovery rates [?];

— Parameters relating to Ssituation awareness parameters (e.g. cue identification, comprehension and, prediction);

— Use of group decision-making methods;

— Gaze time [?] 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 to be used in the reviewverification [?] 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. requirements relating to time constraints, sequence and, precision).[to here]

VALIDATION TESTING

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

— Simulations and test beds should correspond to the design and physical layout of the plant;

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

— The operating tasks should be representative of those used in the plant (e.g. monitoring, detection, diagnosis, anticipation of changes in parameters, surveillance, control and, manual recovery of automatic control systems); [needs to be a should statement like the other bullets]

— The pParticipants should be trained and should occupy a position in the test scenario corresponding to their levels of qualification and responsibility;

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

— The range of human interactions expected during scenarios should be tested. [needs to be a should statement like the other bullets]

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

DATA COLLECTION

5.30. The means of collecting data should be documented in the HFE human factors V&V verification and validation plan. The plan should specify the duration of the number of trials for data tests, the systems and subsystems 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 mockups, field partial task simulators in the field, or and full scope simulators, in order to detect[assess?evaluate?], for example:

— The actions taken by the test participants (e.g. by means of manual collection of data by observers during each test);

— Communication between the test participants in the control room and communication between the control room and other teams involved in the operation of the plant and the crisis management.

5.32. The means of collecting data during the tests should be used to collect Data should be collected on deficiencies, i.e. the detected difficulties and mistakes made by the test participants, and also, on the other hand, to collect data on the ease of use when using theof tools anticipated by the design. Consequently, the validation tests should be used to identify the resources that provide support for operator actions for safety purposes and those for which improvements are necessary, for example:

— To facilitate the surveillance of the plant installation and to enhance the understanding of the situation awareness [?];

— To optimizse the workload of the personnel;

— To encourage coordination cooperation and communications among st the personnel.

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

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

— The chronology of the actions taken;

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

— The identification and analysis of remarkable unusual [remarkable has positive connotations] facts occurrences in the execution of the scenario (e.g. any difficulties encountered by the personnel, hesitations about how to proceed and, 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 reviewanalysis [what review? analysis as in next subsection?].

DATA ANALYSIS

5.36. The analysis of the validation tests requires should [should statement?] involve an in-depth examination of the collected data. It The analysis should cover both the mistakes made by the test participants as well as human activities that were performed successfully. Furthermore, in all the tested operating situations tested, 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 both the analyst and users).

5.37. The analysis of the collected data should justify demonstrate [justify means give reasons for] 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 were able to:

— Comprehend the situation;

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

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

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

5.39. The corresponding solutions applied to mitigation HFE related issues, solutions and their effectiveness of these solutions, 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 performed should be produced that

summarizes the test plan, test findings, suggestions for improvements and conclusions.

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

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

6. HFE DESIGN IMPLEMENTATION

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

6.2. The design implementation phase should be performed as part of the formal build construction [?] 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 whether there are any unforeseen issues that arise when the design is implemented in the actual plant and working 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 organizational [?] conflicts) relating to personnel, safety the management systems, or technological systems, structures or components (e.g. inconsistencies with existing systems or interfaces).

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

— Organizsational factors;

— Personnel factors;

— Job design;

— Safety analysis;

— Probabilistic safety assessment and/ human reliability analysis;

— Human machine interfaceThe HMI;

— Equipment;

— Procedures;

— Training;

— Plant reference documentation;

— The wWorking environment.

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

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

— Elements that need to be in place prior to commencing the implementation, e.g. the training of the implementation team on the use of simulators or test rigs beds [?]training which that is necessary to ensure they attain the desired level of task performance from the implementation team;

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

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

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

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

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

— Any negative effects on the humans, technology and the organizsation are tolerable or suitably ameliorated;

— Any changes made to the as-built HFE design are reflected in plant drawings and materials, e.g. training material, procedures, drawings, simulators, organiszational 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 toplan for resolution has been assignedestablished;[this language is more standards-y]

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

7. HUMAN PERFORMANCE MONITORING

7.1. The mMonitoring of human performance should be an active and on-going process to evaluate the continuing effectiveness of the design to properly support people personnel to carryin carrying out their work tasks safely and effectively. It Monitoring of human performance provides insights into:

— Whether the HMI design meets (and will 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 in accordance with within time response time criteria [OK?] and performance criteria;

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

— Whether the system supporting provisions, 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:[all should statements below?]

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

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

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

— A culture of open and honest reporting should be established to ensureT the effective use of issue reporting by system users in monitoring human performance [OK to delete ‘in monitoring human performance’ – the statement seems broader than just that]needs a culture of open and honest reporting;

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

— A sSufficient flexibility [flexibility in what? in the extent of monitoring? in the acceptance of human performance?] is should be applied proportionate to the risk presented by the deviation in acceptable human performance;[this seems like a graded approach statement, but it is not quite right – we grade the application of safety measures to the consequences (not the risk)]

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

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

7.4. Where applicable, the human performance monitoring should be compatible withIn new build projects where in which the owner/operator operating organization is not the design authority, it should . This is to be ensured that assumptions made during at the design stage phase about human performance are captured and validated during in the licensing commissioning and operational stagesphases.

8. APPLICATION OF HFE IN DESIGN FOR COMPUTERIZED PROCEDURES

GENERAL

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

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

8.3. Computerized procedures should be included in the plant configuration management programme of the plantand administration.[what does 'and administration' mean?]

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

8.5. Computerized procedures systems are of three types:

— Type I systems represent an equivalent reproduction of paper based procedures and do not receive any processed or real-time information;

— Type II systems augment procedures with dynamic embedded process data;

— Type III systems provide the capabilities of Type II systems and included embedded soft controls to manipulate plant equipment. These Type III systems may could include the capability for automated sequences of steps that automatically carry out the described actions described in the procedure.

GUIDELINES FORTHE HMI FOR COMPUTERIZED PROCEDURES SYSTEMS'S HMI

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

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

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

— Continuously provide distinguishing information, e.g. title, revision number, date, plant name and, unit, for each procedure;

— Maintain consistency of display and location of information, navigation aids, controls and other application menus for each display in the computerized procedure system;

— Arrange the computerized procedures system (including, e.g., its structure, format, navigation menus and, controls) to be adaptive to any device on which the system is going to be used.

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

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

INTERACTION WITH THE COMPUTERIZED PROCEDURES SYSTEM

8.10. The following recommendations on interaction capabilities set out in paras 8.11 to 8.20 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 Each warning or caution is presented in a way that is easily distinguished from other warnings or cautions or warnings.

8.12. EachA 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 set of items is clearly distinguished from other sets of items;

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

8.13. The Sstatus 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 aAn indication of alternative action where necessary should also be included.

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

8.15. The computerized procedures system may have Mmultiple procedures within the computerized procedures system being might need to be executed at the same time. [merge paras – the original 8.15 doesn't contain any guidance]

8.16.8.15. In such instances, human resources are should be allocated appropriately and coordination of the execution of multiple procedures should be consideredcoordinated. For example, when more than one procedure is being carried out simultaneously withat the same time as another, the procedure and the progress instatus of steps in [same language as para 8.13?] that procedure should be displayed at on all devices.

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

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

8.19.8.18. The ~~D~~data and logic rules that are ~~evaluated~~ used [I don't think one talks about evaluating rules – rather using rules for evaluating outputs/calculations] by the computerized procedures system should be available to the operator.

8.20.8.19. The computerized procedures system should provide ~~the~~ operators with 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.

8.21.8.20. ~~Operators should be in charge of deciding which procedure needs to be used according to plant status.~~[repeated in next sentence] The ~~C~~computerized procedures system ~~may~~ can suggest ~~what~~ which procedure to use, but the responsibility for this decision should lie~~s~~ with the operators, who should take this decision on the basis of the plant status.[is there a difference between plant conditions and plant status? – both are used, but I've generally stuck with plant status] This applies to Type II and Type III computerized procedures ~~Type II and III~~.

FUNCTIONAL CAPABILITIES OF THE COMPUTERIZED PROCEDURES SYSTEM ~~FUNCTIONAL CAPABILITIES~~

8.22.8.21. The computerized procedures system should notify the ~~user~~ operator when the plant ~~conditions~~ status necessitates proceeding to enter a procedure, to exit a procedure or to transition from one procedure to another.

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

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

8.25.8.24. The computerized procedures system ~~may~~ might automatically process certain steps ~~logic~~ within a procedure ~~(e.g. step succession)~~ [step succession and step logic not mentioned elsewhere in standards and even google doesn't throw those terms up – jargon that could be avoided in here?] and provide this information to the operator. Results of the automatic processing of steps ~~logic~~ should be highlighted to the operator.

~~8.26.~~ The computerized procedures system should indicate those steps (e.g. time-dependent and process-dependent steps) ~~that need~~for which continuous monitoring by the operator is necessary.

~~These may be time-dependent and process-dependent steps that are monitored by the operator.~~ [merge paras, otherwise the 'these' in the next para is confusing]

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

~~8.28.~~8.25. In addition, the computerized procedures system should indicate whether ~~parameter~~ the monitoring of parameters has stopped or is still ~~being continued~~ongoing.

~~8.29.~~8.26. The computerized procedures system, including soft controls to manipulate plant equipment (for~~procedures~~ Type III procedures) should provide the operator with the necessary information to support the effective use of these controls.

DEGRADATION AND FAILURES OF THE COMPUTERIZED PROCEDURES SYSTEM

~~8.30.~~8.27. ~~HFE~~ [HFE is not a person to whom responsibility can be given] ~~should develop g~~Guidelines should be developed for switching to backup procedures (e.g. paper based procedures, and/or backup hardware panels), as well as for switching back from back-up procedures to ~~the~~ computerized procedures when appropriate. ~~it~~ [what is 'it'? "when the computerized procedures system works again~~works again~~?" then you'd have to put in a link earlier in the sentence]

~~8.31.~~8.28. Degraded conditions and failures ~~requiring~~ necessitating a transition to ~~a~~ backup procedures should be recognized and indicated by the computerized procedures system.

~~8.32.~~8.29. Paper based procedures used as backup procedures should be available and accessible to operators.

~~8.33.~~8.30. The structure and format of information in the computerized procedures should be compatible with the structure and format of information in backup procedures.

~~8.34.~~8.31. When a transition to a paper based backup procedure becomes necessary, the following information should be available:

— Procedures ~~which~~ that were currently being carried out;

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

— Information about ~~continuously monitoring~~ steps or conditions that were being monitored when the transition to backup procedures took place;

— The ~~I~~information necessary~~needed~~ to continue the execution of the procedure where it was interrupted, avoiding repetition of steps already completed.

~~8.35.~~8.32. The t~~T~~ime necessary ~~needed~~ to undertake the transition to back-up procedures should be validated as meeting ~~system~~ the functional requirements for the computerized procedures system. [is

this what the 'system functional requirements' are? or is it a different system?]

8.36.8.33. Training on Ccomputerized procedures training should include the specific steps required necessary for the transition to paper based procedures.

AUTOMATIC SEQUENCINGE OF STEPS IN COMPUTERIZED PROCEDURES

8.37.8.34. The Hhighest level of computerized procedures is automatizationautomation [you seem to call it automation elsewhere, or are these different things?], i.e. automated sequences of steps that automatically carry out the described actions described in the procedure. Automation of the sequences of procedure steps is only applicable to procedures Type III procedures.

8.38.8.35. The execution of [pls check – is it the existence of the automated sequences or the application of the automated sequences that is to be authorized and monitored?] aAutomated sequences present in computerized procedures should be authorized and monitored by operators,[pls check if this comma is OK] who are responsible for safe plant operation.

8.39.8.36. Operators should be able to choose either whether to execute the steps of the a computerized [computerized?] procedure manually or to activate the automation.

8.40.8.37. Operators should be in charge ofresponsible for selecting which procedure will be used.

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

8.42.8.39. Information on dDetailed and specific sequences of steps should be indicated provided to operators by the computerized procedures system. [what does indicated mean? displayed on the HMI? what are detailed and specific sequences?]

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

8.44.8.41. Information on fFailures of automation should be indicated provided, along with the point in the sequence when at which failure occurred.

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

Hold points in automated sequences of steps

8.46.8.43. An automated sequence of steps may could include a hold point, which is a predefined point in the procedure at which the procedure needs will halt its progress and request the operator to acknowledge the status of the automated sequence and to authorize the procedure to continue.

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

— Help Assist the operator into recognizinge the progress of the automation and to make any relevant and necessary decisions or/ adjustments for the procedure to continue;

— Keep Maintain the operator's awarenessconscious of the status of plant equipment involved in the sequence of steps being carried out;

— Enable the operator to authorize the procedure to continue.

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

8.49.8.46. Pre-defined hold points should not be allowed to be removed by the operator.

8.50.8.47. Hold points defined in a procedure should leave the procedure in a stable condition [or leave the plant in a stable state?] in which the operator is able to correctly evaluate the status of the procedure and to make the necessary decisions for the procedure to continue.

Interruption of automated sequences of steps

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

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

8.53.8.50. The cComputerized procedures system should be able to automatically interrupt an automated sequence in the event that a necessary 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 cannot be guaranteed for any other reason.

8.54.8.51. The cComputerized procedures system should alert the operator of to any interruption of the an automated sequenceprocedure.

9. HFE INTEGRATION OF HFE IN SAFETY PROCESSES

DEVELOPMENT AND REVIEW OF THE SAFETY ANALYSIS REPORT

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

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

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

— The human factors analysis methods applied;

— Assumptions for the choice of HMI design, with taking into account taken of HFE;[OK?]

— Human factors verification and validation, including the identification and resolution of HFE related issues identified [too many identifieds in this sentence, it seems] during the design project and assumptions made during analysis;

— A description of how the HMI design has been implemented in the overall plant designas a whole; [meaning unclear]

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

9.3. HFE A review should be conducted to determine and [either 'determine whether' or 'verify that' but you can't say both] verify that acceptable HFE practices and guidelines were incorporated into the design and the safety analysis report.

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

9.5. Modernizations and mModifications of the plant in respect of HFE human factors design should be documented in the safety analysis report.

9.6. Guidance Recommendations on the format and content of the safety analysis report is are given provided in IAEA Safety Standards Series No. GS-G-4.1, Format and Content of the Safety Analysis Report for Nuclear Power Plants, 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 A review of HFE aspects [I'm wary of using HFE review because it is not a concept that you have attempted to define early on in the Guide – though it seems like it could be a good concept, you've used it only in a very few places – seems like only some of your authors liked it] should be conducted to identify the potential impact on risk whenever a modification of human tasks results from modernizationsmodifications to the plant, both small-scale andor large-scale modifications, to identify a potential risk impact.

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

9.10. The effect of the plant modifications and modernization on human tasks should be reviewed.[I've tried to distinguish this sentence from para 9.8 but they do seem to be saying much the same thing]

9.11. A graded approach should be applied to tThe HFE programme on for plant modifications and modernization should use a graded approach.

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

9.13. Guidance and rRecommendations on controlling activities relating to modifications at to nuclear power plants are provided in IAEA Safety Standards Series No. NS-G-2.3, Modifications to Nuclear Power Plants Ref. [14].

PERIODIC SAFETY REVIEW PROCESS[OK?]

9.14. Thise clauses in this section provides guidance recommendations on HFE activities that can support the intent of IAEA Safety Standards Series No. SSG-25, Periodic Safety Review for Nuclear Power Plants Ref. [15].

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

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

— The feasibility of the division and coordination of work in the most resource intensive conditions is feasible, through as assessediding by 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 necessary needed for successful human performance during are suitable and sufficient for the most resource intensive conditions are suitable and sufficient.[need to say suitable and sufficient for what]

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 in respect of human tasks identified in safety analyses, continue to be valid.

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

9.19. The periodic safety review should be used to identify reasonably practicable improvements in managing human and organizational factors to ensure that sufficient successful [sufficient seems a bit weak – elsewhere you talk about successful human performance, or also about optimizing human performance] human performance is achieved, including through the HFE programme.

10. APPLICATION OF HFE IN PRODUCT SELECTION AND PROCUREMENT

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

USE OF PERSONAL PROTECTIVE EQUIPMENT

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

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

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

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

COMMERCIAL OFF THE SHELF PRODUCTS

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

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

— Within each system;

— Between similar systems that are already used by operators;

— With existing characteristics of the HMI at the workstation.[or do you mean plant rather than workstation?]

10.8. Where a commercial off the shelf COTS product is integrated withto be incorporated into an existing system, the impact on human performance should be assessed. [OK? as integrated with might mean interfacing with]

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

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

MOBILE DEVICES

10.11. The scope of the HFE review of mobile devices should [?] includes hand held, portable, and wearable devices.

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

10.13. Mobile devices and their characteristics should be selected and to be compatible with the users' anthropometrybody sizes, the 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 they are not in use.

10.15. Where appropriate, information regarding requirements for mobile devices in extreme environments (e.g. the use of rugged devices) should be provided to users [what does provided mean?].

10.16. The Sstorage of the hand held mobile devices should be considered in HFE evaluationsanalyses.

10.17. HFE should consider Rrequirements for the synchronization or calibration of mobile devices that may be unique to this form of interfaceshould be considered.[what does the deleted part mean? what form of interface?]

10.18. For mobile computing devices, error management is of high importance for safety due tobecause of the potential constraints of on 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 and, correction offor correcting individual

errors without requiring the need for re-entry of correctly entered commands or data elements to be re-entered);

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

— Error checking in a manner that does not disrupt the user (e.g. 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 is controlled from a mobile device (e.g. capability to stop the process at any point in the sequence as a result of an indicated error).

10.19. The potential for interference from high intensity radiated radiation fields should be considered and as these 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~~Operating Experience ~~from Events in~~Feedback for Nuclear Installations, IAEA Safety Standards Series No. ~~NS-G-2.11~~SSG-50, ~~[[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). (A revision of this Safety Guide is in preparation).~~[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 NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna (2009). (A revision of this Safety Guide is in preparation).

[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, IAEA, Vienna (2004). (A revision of this Safety Guide is 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

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

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

AI–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 SSR-2/1 (Rev. 1) Ref. [AI–1]. It is expected that designers, users operating organizations and regulatory bodies will take advantage of the information in these standards.

AI–3. Two standards development organizations are responsible for most of the internationally used standards for instrumentation and controlI&C systems in nuclear power plants: the International Electrotechnical Commission's (IEC's) Subcommittee 45 (SC45A) and the Institute for Electrical and Electronic Engineers' (IEEE's) 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 SSR-2/1 (Rev. 1) Ref. [AI–1] and the recommendations of this Safety Gguide. Consequently, either set of standards can be used to further interpret the recommendations of this Safety Guide.

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

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

AI–64. 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.

AI–75. Nevertheless, users need to recognize and take account of the fact that there are important differences between the IEC and the IEEE standards. [merge paras]

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.

AI-87. IEEE standards focus largely on items important to safety-items and, therefore, the-ir IEEE guidance directly applies to a smaller set of functions, systems and equipment than this Safety Guide does. Nevertheless, the guidance of the IEEE can be applied to safety related items (items important to safety that are not safety systems) using a graded approach.

AI-98. 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 also relate to the major topical areas of this Safety Guide-as well. Table AI-2 shows how other guidance documents relate to the major topical areas of this Safety Guide.

TABLE AI-1 INTERNATIONAL STANDARDS HAVING A STRONG RELATIONSHIP TO WITH 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[22]

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 AI–2 RELATIONSHIP BETWEEN INTERNATIONAL STANDARDS, RELEVANT GUIDES AND THE TOPICAL AREAS OF THIS SAFETY 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. Application of HFE in Ddesign	
– 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 pParameter dDisplay sSystems	IEC 60960, IEEE 497 (in revision), NUREG 0700, NUREG-0696
– General principles relating to HFE~~human factors engineering~~ for I&C systems	IEEE 1023, IEEE 1082, IEEE 1289
5. ~~Human Factors~~ Verification and vValidation in respect of human factors	NUREG-0711, Rev. 3
6. Implementation of the design	IEC 61839, IEEE Std 845, IEEE 1082, NUREG–0711, Rev. 3,
7. Human pPerformance mMonitoring	IEEE Std 845, NUREG–0711, Rev. 3
8. HFE IIntegration in safety processes	IEC 61772, IEC 62241, IEEE Std. 1289, NUREG–0711, Rev. 3
– General principles relating to HFE~~human factors engineering~~ for I&C systems	IEC 61513, IEEE 1023, IEEE 1082, IEEE 1289
– Computerized procedures	IEC 62646, IEEE 1786

REFERENCES TO THE ANNEX I

[A1–1] 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 a definition that differs from that provided in the IAEA Safety Glossary.*

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

computerized procedure system. A sSystem 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.[this appears only once in the text – do you need to list it here?]

human -machine interface (HMI). The human-machine interfaceHMI is that the part of the a [what system?] system through which personnel interact with the system to perform their functions and tasks. The HMI is constitutesd the by interface between staff personnel and plant systems, including procedures, communication systems displays, alarms and controls.

human motor control. Human mMotor control is the physiological capability of a human's muscular system that is able to control movement, including strength and fine movements.[this appears only once in the text – do you need to list it here?]

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.~~[not used in the text]

important human tasks.: Human tasks that may can have an adverse or positive effect on operational safety,[we don't talk about operational safety as something distinct from safety] as determined by safety analysis.

situation awareness. The dynamic process of perception and comprehension of the plant's actual [or current?] plant's condition in order to support the ability of individuals and teams to predict the future systems conditions of systemsby 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 [in the first sentence it appears that plant conditions and actual conditions are the same thing – so what does it mean to say there is a difference between them?] 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 means of objective evidence that the HMI system as a whole [?] meets the design specifications, requirements and provides the support necessary needed to accomplish tasks, as intended.

validation.* Confirmation by examination and by provision means of objective evidence to ensure that the HMI system as whole [?], including the user, can successfully perform that system'sits intended functions and meet its, goals and objectives in the anticipated range of operational environments in which it is anticipated to have to operate.

CONTRIBUTORS TO DRAFTING AND REVIEW

[no Gary Johnson? I thought I could detect his writing style here … ☺]

Duchac, A.	International Atomic Energy Agency
Gertman, D.	Idaho National Laboratory, United States of America
Hata, T.	Nuclear Regulation Authority, Japan
Humbel, C.	Swiss Federal Nuclear Safety Inspectorate, Switzerland
Illobre, F.	Tecnatom, Spain
Ito, K.	MHI Nuclear Systems and Solution Engineering, Japan
Johansson, Y.	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