IAEA Nuclear Energy Series

No. NR-T-2.12

Human Factors Engineering Aspects of Instrumentation and Control System Design

IAEA
International Atomic Energy Agency

IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A.3 and VIII.C of its Statute, the IAEA is authorized to "foster the exchange of scientific and technical information on the peaceful uses of atomic energy". The publications in the **IAEA Nuclear Energy Series** present good practices and advances in technology, as well as practical examples and experience in the areas of nuclear reactors, the nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues relevant to nuclear energy. The **IAEA Nuclear Energy Series** is structured into four levels:

(1) The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.
(2) **Nuclear Energy Series Objectives** publications describe what needs to be considered and the specific goals to be achieved in the subject areas at different stages of implementation.
(3) **Nuclear Energy Series Guides and Methodologies** provide high level guidance or methods on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.
(4) **Nuclear Energy Series Technical Reports** provide additional, more detailed information on activities relating to topics explored in the **IAEA Nuclear Energy Series**.

The IAEA Nuclear Energy Series publications are coded as follows: **NG** – nuclear energy general; **NR** – nuclear reactors (formerly **NP –** nuclear power); **NF** – nuclear fuel cycle; **NW** – radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA web site:

www.iaea.org/publications

For further information, please contact the IAEA at Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of the IAEA Nuclear Energy Series publications are invited to inform the IAEA of their experience for the purpose of ensuring that they continue to meet user needs. Information may be provided via the IAEA web site, by post, or by email to Official.Mail@iaea.org.

HUMAN FACTORS ENGINEERING ASPECTS OF INSTRUMENTATION AND CONTROL SYSTEM DESIGN

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

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

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

IAEA NUCLEAR ENERGY SERIES No. NR-T-2.12

HUMAN FACTORS ENGINEERING ASPECTS OF INSTRUMENTATION AND CONTROL SYSTEM DESIGN

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

COPYRIGHT NOTICE

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

Printed by the IAEA in Austria
March 2021
STI/PUB/1919

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Human factors engineering aspects of instrumentation and control system design / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA nuclear energy series, ISSN 1995–7807 ; no. NR-T-2.12 | Includes bibliographical references.
Identifiers: IAEAL 20-01380 | ISBN 978-92-0-121520-8 (paperback : alk. paper) | ISBN 978-92-0-121620-5 (pdf) | ISBN 978-92-0-121720-2 (epub) | ISBN 978-92-0-121820-9 (mobipocket)
Subjects: LCSH: Nuclear power plants — Instruments. | Nuclear reactors — Control. | Nuclear power plants — Human factors. | Human engineering.
Classification: UDC 621.039.56 | STI/PUB/1919

FOREWORD

The IAEA's statutory role is to "seek to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world". Among other functions, the IAEA is authorized to "foster the exchange of scientific and technical information on peaceful uses of atomic energy". One way this is achieved is through a range of technical publications including the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series comprises publications designed to further the use of nuclear technologies in support of sustainable development, to advance nuclear science and technology, catalyse innovation and build capacity to support the existing and expanded use of nuclear power and nuclear science applications. The publications include information covering all policy, technological and management aspects of the definition and implementation of activities involving the peaceful use of nuclear technology.

The IAEA safety standards establish fundamental principles, requirements and recommendations to ensure nuclear safety and serve as a global reference for protecting people and the environment from harmful effects of ionizing radiation.

When IAEA Nuclear Energy Series publications address safety, it is ensured that the IAEA safety standards are referred to as the current boundary conditions for the application of nuclear technology.

Safe, reliable and productive performance in the nuclear industry results from a systematic consideration of human performance. A plant or other facility consists of both the engineered system and the human user of that system. It is therefore crucial that engineering activities consider the humans who will be interacting with those systems. Engineering design, specifically instrumentation and control (I&C) design, can influence human performance by driving how plant personnel carry out work and respond to events within a nuclear power plant. As a result, human–system interfaces (HSIs) for plant operators as well as the maintenance and testing of the I&C system cannot be designed by isolated disciplines.

The focus of this publication is to integrate knowledge from the disciplines of human factors engineering (HFE) and I&C to emphasize an interdisciplinary approach for the design of better HSIs and consequently improved human performance in nuclear power plants. This publication provides practical explanations of the HFE processes and corresponding outputs that inform the I&C development.

The framework outlined in this publication takes into consideration the I&C life cycle described in IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants, and the HFE programme guidance in IAEA Safety Standards Series No. SSG-51, Human Factors Engineering in the Design of Nuclear Power Plants, for easing the inclusion and application of these two disciplines within an engineering design process. This publication specifically addresses points in the design process where collaboration between HFE, I&C and other important disciplines and stakeholders is paramount, and it identifies key tools and tasks for exchanging inputs and outputs between different design disciplines, particularly I&C and HFE.

The primary intent of this publication is to provide Member States with practical information to improve their approach to I&C through the consideration of HFE. This publication may also be useful to design and technical support organizations, as well as to regulatory authorities, by providing background information to support their activities.

The publication was produced by a committee of international experts and advisors from numerous countries. The IAEA wishes to acknowledge the valuable assistance provided by the contributors and reviewers listed at the end of this publication, especially the contribution made by C. Ngo (Canada) and J. Naser (United States of America) as the co-chairs of the authoring group. The IAEA officer responsible for this publication was J. Eiler of the Division of Nuclear Power.

EDITORIAL NOTE

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this book and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Nuclear power plant personnel play a vital role in the safe, efficient and productive generation of electrical power. Operators monitor and control the plant to ensure it is functioning properly. Test and maintenance personnel help ensure the equipment is functioning properly and restore components when malfunctions occur. Personnel performance and the resulting plant performance are influenced by many aspects of plant design, including the instrumentation and control (I&C) systems and the human–system interfaces (HSIs) provided for personnel to interact with the plant. Information presented to plant personnel through I&C systems and HSIs has to be accurate, sufficient, operationally relevant, timely and dependable.

HSIs can have different characteristics depending on the technologies installed in the plant. The general operational and maintenance environment for nuclear facilities is becoming more computer based, incorporating features such as soft controls, computerized procedures, mobile interfaces and touch screen interfaces. These interfaces affect the ways that humans operate and maintain the plant.

While HSI design and digitalization can greatly improve personnel and plant performance, it is important to recognize that, if poorly planned, designed or implemented, there is the potential to negatively impact performance and safety as well as to reduce human reliability, resulting in a detrimental effect on safety and cost-effective power production. Human factors engineering (HFE) is needed to ensure that the benefits of the technologies are realized and problems with its implementation, operation and maintenance are minimized. The I&C systems can consequently affect HSI design and, likewise, HFE can drive some aspects of I&C systems.

IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [1], recognizes this interdependency and the need for integration between I&C and HFE by providing high level guidance for considering HFE inputs into the I&C life cycle and general guidance for HSI design.

IAEA Safety Standards Series No. SSG-51, Human Factors Engineering in the Design of Nuclear Power Plants [2], further expands on the application of HFE by outlining a structured, systematic approach for the development of HFE requirements and inputs into nuclear power plant design and also provides more guidance on HSI design for I&C systems and non–I&C HSIs.

Both SSG-39 [1] and SSG-51 [2] provide recommendations about what should be done in the areas of HFE and HSI design to meet the requirements established in IAEA Safety Standards Series No. SSR-2/1, (Rev. 1), Safety of Nuclear Power Plants: Design [3], SSR-2/2, (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [4] and GSR Part 4, (Rev. 1), Safety Assessment for Facilities and Activities [5]. This publication is intended to supplement the guidance found in the safety standards to provide best practice techniques for how to realize and implement these recommendations.

1.2. OBJECTIVE

The objective of this publication is to provide the design team, which includes I&C and HFE disciplines, with practical implementation strategies and methods for I&C development that will result in HSIs that successfully support plant personnel functions and tasks.

It is not expected or necessary for the I&C engineer to become an HFE expert or for an HFE expert to become an I&C engineer. The intent of this publication is to bring awareness to both I&C and HFE disciplines about the important interactions and techniques in design that are employed to achieve

successful HSI design. This publication is written primarily for the I&C team. Nevertheless, all experts involved in the field of HSI design, analysis, development, manufacture, modification, verification, validation and licensing, as well as general audiences who intend to learn about the process, will find the practices described here useful.

1.3. SCOPE

This publication addresses proposed I&C systems, components and replacements that support HSIs in various nuclear applications, which include new build designs and modifications to existing power plants in operation and decommissioning. This publication covers all I&C systems. Throughout this publication, the term 'I&C system' refers to any I&C system introduced into the design of the plant.[1] This term applies to both I&C systems important to safety and I&C systems that are not. Furthermore, the term HSI is used in this publication to mean the HSI as a part of the I&C system.

The publication contains guidance that is useful for each stage of the I&C life cycle, such as new I&C system design, operation and maintenance, modernization and decommissioning of the I&C system(s). Additionally, it should be noted that the concepts covered in this publication often tend to focus on control room design. However, these concepts can also be applied, through a graded approach, to HSIs outside of control rooms. Some I&C systems may have an HSI in one or each of the on-site control rooms; some may have an HSI in one or each of the off-site support centres; some of the HSIs could also be located in the field.

For significant modernization (including a change of technology) or local modification of existing I&C systems, the publication provides methods for analysis and evaluation of the HFE related design aspects with the intent of providing input into the design of the HSIs for an engineering project. Additionally, the publication provides new I&C engineers with practical techniques to incorporate inputs from HFE analyses such as functional analysis, control function allocation and task analysis. Also, the publication briefly describes where the I&C team can find the HFE related requirements and how to ensure that these requirements are taken into consideration in I&C systems.

This publication was written primarily to raise awareness for those who are responsible for I&C systems with an HFE implication. Such persons are referred to as I&C engineers within this publication. Furthermore, the emphasis throughout the publication is on a team based approach that engages important operations and maintenance stakeholders. The publication specifically addresses points in the development process where collaboration is paramount and identifies key tools and tasks for exchanging inputs and outputs between I&C and HFE disciplines.

This publication is intended to complement other existing IAEA publications, particularly SSG-39 [1] and SSG-51 [2] and is written to minimize overlap with these publications in the following areas:

— The I&C life cycle and development process;
— The development and expectations of an HFE programme.

This publication does not provide detailed, comprehensive guidance on HFE programme development and implementation or on HSI design. The main subject of the publication is to summarize accumulated practical experience to help I&C engineers. Where useful, this publication provides appropriate references for HFE methodologies or HSI design guidance that represents industry best practice and experience.

[1] Note: The term 'I&C system' is used throughout SSG-39 [1] to mean any I&C system important to safety.

1.4. STRUCTURE

The structure of this publication loosely follows the typical sequence of an I&C project.

Section 2 focuses on the development of the end point vision, including the concept of operations, the HSI concept development and HFE programme planning.

Section 3 focuses on the alignment of I&C architecture with HSI design basis requirements and on identifying and specifying the constraints on, and drivers for, the design.

Section 4 provides practical tools for the analyses and considerations for the development of input from HFE analyses that can affect I&C system design.

Section 5 describes an approach for how HSI design can progress within an I&C project. This section takes input from the previous sections and provides guidance specifying HFE considerations for I&C.

Section 6 highlights the development of HFE guidelines that can be used as input in the selection of commercial or modified off the shelf products.

Section 7 takes the reader through best practices for verifying and validating that the I&C system and consequently the HSI meet the HFE requirements.

An example of how these sections integrate into the overall I&C life cycle along with suggested inputs and outputs can be seen in Fig. 1.

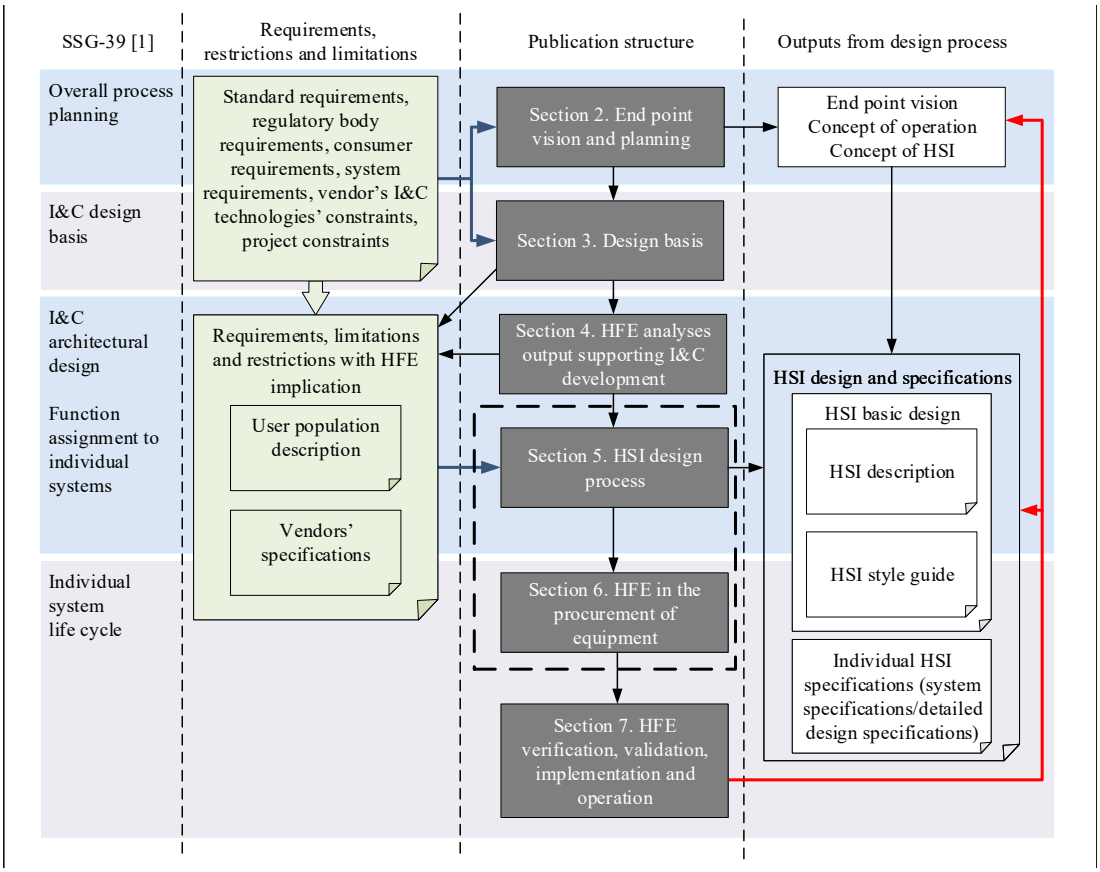


FIG. 1. Structure of a publication with I&C related HFE activities. HFE — human factors engineering; HSI — human-system interface; I&C — instrumentation and control.

The structure of this publication reflects the HSI development process in a step by step manner, starting from the planning of HFE activities and finishing with verification, validation and implementation of the HFE design solutions. This process is consistent with the one described in SSG-39 [1]. To show this relationship, the publication sections that are shown in dark boxes are mapped to the related stages of the I&C life cycle outlined in SSG-39 [1] (the stage titles are shown in the left hand column of Fig. 1).

All requirements, constraints and limitations to be considered during HSI design are shown in the second column on Fig. 1. HFE requirements are extracted from standards, regulatory bodies and other relevant documents at the stage of 'I&C system design basis' development. The requirements are complemented by the results from HFE analyses as well as by information concerning potential I&C system users gathered at the stage of 'HFE analysis inputs into I&C'. All the requirements are harmonized with each other (a process that identifies and reduces potential conflicts of requirements) and used as an input for 'HSI design process and specification'. Requirements specific for particular systems together with specifications of equipment and software provided by vendors are submitted as input for 'HFE in the procurement of equipment'.

The column to the far right of Fig. 1 identifies typical outputs from the HSI design processes. Even though 'HSI detailed design' is not a subject of this publication, it is shown in the Figure to demonstrate the necessity to verify and validate the design solutions proposed at the stage of detailed design.

The purpose of Fig. 1 is to provide some context to the structure and content of this publication and as a result, the Figure reflects a simplification of the design process. The design process can often be non-linear with multiple iterations of activities as design concepts mature. This is not depicted in the Figure for practical purposes; however, it has to be considered a reality in the development of HSIs.

Section 8 summarizes the main technical observations made in this publication.

An appendix and three annexes are attached at the end. The Appendix provides supplemental guidance on select HSI design topics. Annex I details HSI induced cognitive error and cognitive workload analyses. Annex II gives supplemental guidance on HSI design. Annex III discusses HFE verification and validation (V&V) methodologies and acceptance criteria.

2. END POINT VISION AND PLANNING

2.1. INTRODUCTION

This section provides information on the end point vision and HFE planning. It describes the intent of an end point vision for an engineering project and gives practical guidance for its development. It also describes the suggested contents of an HFE programme management plan, giving practical guidance for its development as well as identifying specific considerations relevant to engineering projects.

2.2. CONTEXT AND OBJECTIVES OF AN END POINT VISION

The end point vision's main objective is to provide a clear, overarching description of where an engineering project will ideally end as far as the I&C architecture and the HSIs are concerned, as well as how to operate them. The end point vision defines the overall strategic goals of the project at the level of the overarching project owner (e.g. license holder). As a consequence, the end point vision is the starting

point of an engineering project[2] and it may include a definition of a problem or design shortfall that needs a design solution to resolve it.

The end point vision needs to be a high level, overarching document that guides and informs a project's life cycle and forms a key input into the planning, analysis, design, procurement and V&V activities. Consequently, the end point vision will:

— Need to provide the planned state of the integrated I&C after all the anticipated activities within an engineering project (including I&C engineering activities) are successfully accomplished;
— Guide the engineering activities of projects throughout the design life cycle and support the consistency of the development by ensuring that the I&C systems, specifically their HSIs, are compatible, usable and achieve the project intent;
— Serve as an important communication device as it provides all the project participants and stakeholders with a shared understanding of what the objectives of the project are.

The end point vision needs to be developed by all the stakeholders of an engineering project, including but not limited to the I&C and HFE teams, taking into consideration the whole plant design, construction, commissioning, operation, maintenance and decommissioning.

The end point vision is a key document for all project stakeholders, as many of the requirements to be developed in the design basis and other key documents, such as engineering and human factors (HF) plans, will be derived from it. Close cooperation among all project stakeholders has to be sought during the definition of its content: level of automation, conceptual aspects of the HSI, control rooms concepts and so on. Several examples of such cooperation are included in the rest of this section.

When developing the end point vision, a systematic approach to defining 'who', 'what', 'where', 'when', 'how' and 'why' is important. The end point vision is comprised of the concept of operations and the HSI conceptual design. More information on the development of the conceptual HSI design can be found in Section 2.2.1.1 and more information on the concept of operations can be found in Section 2.2.1.2.

It is important to acknowledge that the end point vision may need to evolve over time. Therefore, the end point vision, and the associated plans necessary to achieve it, need to be flexible to accommodate any important changes. Changes can occur in, for example, plant conditions, budgets or priorities, and new technologies can emerge that would necessitate a change to the end point vision. Additionally, lessons and experience learned from other projects can also necessitate a change.

Making updates to or changing the end point vision needs to be done at relevant and appropriate design phases according to the needs of the project. The purpose of the update has to be to consider whether the initially planned design solution was feasible and amend the end point vision if necessary. It is also important to ensure that all changes from the original design intent are recorded to ensure that there is an accurate historical record of any project changes.

The following initial project considerations and strategic goal examples can be used as inputs into the development of the end point vision:

— Licensing environment considerations;
— Staffing (depending on reactor type, modification type, plant conditions), overall roles of staff members, required level of competence for each role;
— Measures to maintain staff competence, considering plant condition awareness and training;
— Maintenance and renovation of HSI systems;
— Commercial and economic considerations;
— Technology employed and desired level of automation;
— Defence in depth and safety classification.

[2] In this document, 'engineering project' is understood as the 'I&C and HF engineering project'.

It is important to recognize that developing the end point vision needs a multidisciplinary approach. Figure 2 shows the interactions between HFE and I&C disciplines. The combined I&C and HFE team needs to conduct cross reviews of individual requirements of mutual concern, then generate harmonized requirements/conclusions for common technical areas, such as the level of automation.

2.2.1. Scope of end point vision

The scope of the end point vision is defined by the strategic goals, HSI concept and concept of operations. The end point vision will help to define the scope of the engineering project by defining the need for I&C solutions and by outlining the high level activities, stakeholders and interfaces required to achieve it. An end point vision scope will depend on the type of engineering project (e.g. new build or decommissioning) and may contain, but not be limited to, the following:

— A high level statement of need or objective;
— A definition of key stakeholders;
— A definition of key interfaces (e.g. with other equipment, personnel, design teams);
— A high level definition of potential solutions and, if applicable, procurement strategy.

The end point vision typically comprises the following two components, which are discussed in more detail on the following pages:

— HSI conceptual design;
— Concept of operations.

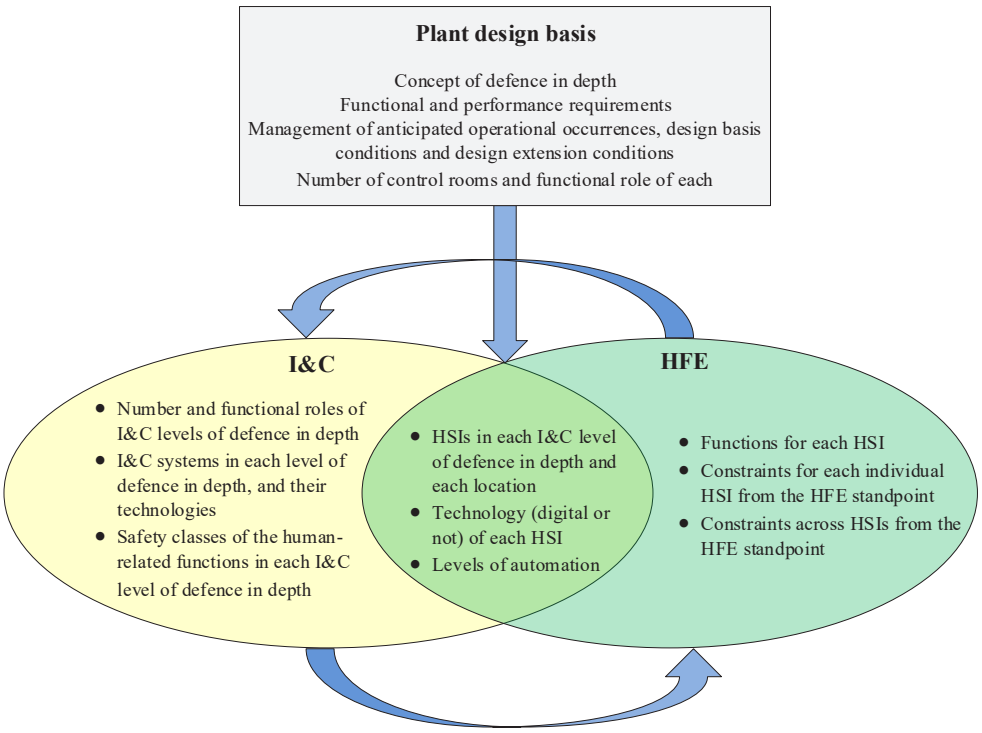


FIG. 2. Example of interactions between I&C and HFE. HFE — human factors engineering; HSI — human-system interface; I&C — instrumentation and control.

2.2.1.1. Human–system interface conceptual design

The HSI conceptual design will typically start by determining:

— The *where*: The geographical and physical locations of the HSIs and HSI components.
— The *which*: The known HSIs and HSI components. This will often be determined based on the I&C architecture and the list of locations.
— The *who*: The intended users of each HSI or HSI component. This will often be determined based on overall staffing decisions.
— The *when*: When a given HSI or HSI component is to be operated, relative to the main plant state and conditions.
— The *what*: The main functions and their main characteristics to be provided by each HSI or HSI component (e.g. alarm management or computer based procedures (CBPs)), possibly depending on the 'when'.
— The *how:* Expectations on HSIs or HSI components usage, operation and maintenance in a given environment.

At this stage, the emphasis is on 'concepts' and avoidance of system design or implementation. The purpose is to provide an overall picture that will be refined by the concept of operations and the HSI conceptual design.

Advice from HFE experts has to be sought when defining the scope of the conceptual design as well as providing input to optioneering or other design selection activities. For instance, from an I&C point of view, to ensure safety of the plant, the HSIs belonging to different levels of defence in depth have to be independent and diverse from one another. From an HF point of view, mixing different HSIs that may look and behave differently (but provide the same function) may be detrimental to human performance, increase the potential for human error and pose safety issues. The HSIs used to monitor and control each aspect of the plant condition have to be consistent with each other and with the rest of the plant (i.e. the same functions and operation across the plant). Thus, a trade-off between these two opposite requirements has to be sought with appropriate justification that it is acceptable to each concerned party.

The HSI conceptual design also needs to describe the degree of automation and the maintenance strategy desired, as these will affect how the engineering project is scoped and defined, and will have major impacts on both I&C and HFE. From an I&C point of view, more automation or equipment monitoring can introduce more physical equipment in some instances, such as sensors, cabling, cabinets and racks, and thus can be more expensive and require more physical space. From an HFE perspective, many requirements have to be met to ensure good integration between plant personnel and automation, which, in turn, can induce extra I&C costs. Additionally, defining the tasks required to interface with automated systems requires an in-depth definition and allocation of function of human tasks that, in turn, will have major impacts on staffing, training and qualifications of plant personnel. Developing and defining a common understanding between HFE and I&C experts on the level of automation and equipment monitoring is thus inevitable.

The following paragraphs provide example content for HSI conceptual designs.

For new builds, the HSI conceptual design describes the different HSIs and HSI components and the different control locations relevant for plant operation. In this case, the conceptual design needs to consider as a minimum:

— The main control room (MCR);
— Supplementary control room(s);
— The technical support centre;
— Other relevant facilities for plant operation, such as those for emergency management, fuel handling or local control stations;
— The locations of I&C equipment.

One could also take account of other centres such as security monitoring centres, remote equipment monitoring centres and also non-fixed locations, such as mobile HSIs assigned to field operators. For design modifications, the HSI conceptual design describes those HSIs or control centres applicable to the modification.

Both for new builds as well as for design modifications, the HSI conceptual design descriptions consider as applicable:

— The layout of HSI panels and workstations within the control centres, considering the use of screens or panels/desks, with all the necessary hardwired indications and controls (this could determine the size of the control centre).
— The technological approach within the control centres. A cockpit approach relies more on digital technology using a certain number of screens to view/use all the necessary information and controls, compared to the analogue approach, where all controls and indications are present in a console/panel/centre concept.
— The locations of I&C equipment.

2.2.1.2. Concept of operations

SSG-51 [2] regards a concept of operations document as an essential requirements input document for an engineering project. SSG-51 [2] defines the concept of operations document as a description of "the proposed design in terms of how it will be operated to perform its functions, which includes the various roles of personnel and how they will be organized, managed and supported. The concept of operations describes how the plant is operated ('operating philosophy') and includes aspects such as the number and composition of operating personnel and how they operate the plant under normal and abnormal conditions."[3] It is designed to 'communicate a story' of when and why and by whom the design is used throughout its life. It is therefore considered highly beneficial, not only for the design or acquisition of new systems, but also for the operation of the system after implementation.

The development of the concept of operations usually requires a team based approach, which may include plant managers, HFE experts and engineers from different departments who can provide valuable experience about the performance of existing designs (including the technological approach, maintenance problems, ageing problems) as well as end users who provide experience in the use of HSIs. End users can identify those HSI features to be avoided and provide useful information from experience of existing systems that can inform the development of the system specifications. Finally, vendors provide input into the concept of operations through their knowledge of the capabilities of the I&C and HSI to be supplied.

[3] The ISO/IEC/IEEE 29148 standard [6] defines the concept of operations (ConOps) document as a "verbal and graphic statement, in broad outline, of an organization's assumptions or intent in regard to an operation or series of operations." In a further explanation the standard adds: "The concept of operations provides the basis for bounding the operating space, system capabilities, interfaces and operating environment." Note that the ISO/IEC/IEEE 29148 standard [6] also defines a system operational concept (OpsCon) document, and the existence of the two (i.e. ConOps and OpsCon) may result in some confusion. As per the standard, the operational concept document "describes what the system will do (not how it will do it) and why (rationale). An OpsCon is a user-oriented document that describes system characteristics of the to-be-delivered system from the user's viewpoint. The OpsCon document is used to communicate overall quantitative and qualitative system characteristics to the acquirer, user, supplier and other organizational elements." The current document does not make the same distinction and the intent of the concept of operations used within this document embodies both the ConOps and OpsCon defined in ISO/IEC/IEEE 29148 [6].

The concept of operations typically refines the 'who' and 'when' of Section 2.2.1.1 and also answers the 'why'. For example:

— *Who:* Description of HSIs, including human-to-human and human-to-system interactions, based in particular on the number of personnel who will have plant monitoring and operational control responsibilities on each shift (i.e. 'control personnel') and staffing levels for these personnel across shifts.
— *When:* Description of activities, tasks, flows, precedence, concurrencies (time/sequence related elements necessary to achieve mission objectives in various product modes and conditions). It includes other mechanisms that enable or support control personnel responsibilities for monitoring, disturbance detection, situation assessment, response planning, response execution and the management of transitions between automatic and manual control.
— *Why:* Rationale to clarify the reader's understanding of specific events found in operational concept scenarios.

The concept of operations describes the characteristics of a new or existing system from the viewpoint of people who will use that system, while communicating the quantitative and qualitative characteristics of the system to all stakeholders.

The concept of operations scope is defined to be relevant to the engineering project being considered, including descriptions of all the plant conditions and the personnel and their roles associated with the operation. Importantly, the concept of operations is drafted in conjunction with HSI conceptual design and these two documents form the overall picture or end point vision of the design solution.

The description of plant conditions within the concept of operations scope includes the staffing necessary for the various locations involved in plant operation (or any other relevant activity), as well as the type and format of applicable procedures to be followed. Considerations for staffing and planned procedures at this stage are still assumptions that need to be evaluated further as the design progresses. The following paragraphs provide examples of the content of the concept of operations for different applications.

For design modification or a modernization programme, the scope is relevant to what is being modified or modernized in terms of plant conditions, control centres and other locations, HSI or specific systems added or modified, as well as the personnel roles involved in the operation (generic examples of design modifications include equipment replacement, architecture update, integration and automation).

Fundamentally, the concept of operations has to provide information on the overall approach and the context of any transitions between different plant conditions that are needed.

In the case of a new system as part of a design modification, this description could be limited to a single operator in charge of one or several systems, although many alternatives could be possible, depending on the modification.

As an example, the content of a concept of operations could contain the following information:

— The main high level tasks or duties to be performed for each crew member for each location and the associated HSI. Examples of tasks to be included, among others, and for each plant condition, are:
    - Plant operation and monitoring during normal operation;
    - Plant operation and monitoring during transients and accident conditions (including global accident management);
    - Management of alarms under all plant conditions;
    - Coordination of all plant operators, including MCR operators, local operators, emergency facilities operators/members (e.g. technical support centre, emergency support centre, maintenance people during all modes of plant operation);
    - Enforcement of proper fulfilment of operating and administrative routines;
    - Authorization, supervision and performance of maintenance operations.

— Description of the concept of operations scope, which may include:
  - Transitions between different plant conditions using the conceptual HSI;
  - Degraded I&C condition or HSI failures (e.g. loss of alarm processing, loss of alarm display, loss of controlling interface, loss of CBPs, planned contingency actions with HSI conceptual design).
— Description of anticipated failures of the I&C system impacting HSI, which may consider:
  - Means to detect and confirm the failure;
  - When the plant can be maintained in operation until the I&C failure is resolved;
  - When the plant needs to be taken to shutdown;
  - Actions within a contingency plan to solve the I&C failure;
  - Actions within an emergency plan to mitigate the I&C failure.

When considering the concept of operations, it is also important to consider how the 'concept' will be maintained. For instance, if a predictive or conditional approach to maintenance is sought, more data coming from equipment (actuators, sensors, etc.) have to be processed by the I&C. This will have an impact on the architecture of the I&C of the plant. From an HF point of view, it is necessary to define who will analyse the data and the HSI needed to do this. Thus, I&C and HFE experts have to agree on the type of maintenance that is sought (e.g. periodic maintenance versus condition based maintenance) and the level of automation to be provided, such as:

Will the system process and assemble the data and just display the information to the operators?

Or, will the system monitor all the data from the equipment and send an alert to plant personnel when a specific threshold is reached?

Each option has pros and cons from an HFE and I&C point of view. From an HFE perspective, this also raises questions about the level of qualification and skills people must have to monitor such data. It is important to recognize that a concept of operations document can help to shape the specification and design of the HFE analyses and the HFE analyses may also serve to refine and modify the concept of operations. A formal concept of operations document may not be required for all design activities but keeping in mind the general concept of operations (a focus on the end user of the system) ensures that the outputs of the HFE analyses are useful to optimize the I&C implementation.

2.2.2. Specific considerations for developing the end point vision

2.2.2.1. End point vision location specific considerations

The design of an I&C system supporting HSIs needs to be considered in the context of the technologies found at each location. Consistency of look, feel and function is important to ensure that the potential for operator error is minimized.

For modernization efforts of existing locations, the end point vision plays a crucial role in preventing fragmentation of the HSI. Fragmentation between old and new systems could be the result of inconsistencies between old, existing systems and the new 'concept' system. The end point vision would aim to identify the interfaces between the old and new systems and determine how the end design would mitigate any design inconsistencies that would result from integrating an old and a new design. Cost efficiencies can be realized by anticipating future upgrades and considering them in conceptual design planning.

In modernization programmes, an end point vision can benefit from integrating a phased approach to the implementation of the modifications while considering all the necessary anticipated changes. For example, in the modernization of an active working control centre, upgrades may proceed in a stepwise fashion, one system at a time, often corresponding to successive outages. In this phased approach, the end point vision helps to ensure that upgrades proceed in a systematic fashion and maintain consistency across each step of modification implementation. (A stepwise V&V check can also help to ensure this.)

2.2.2.2. Evaluating technology options

The first step of evaluating technology options is to identify any available technologies that realize the desired concept of operations and HSI concept design. For example, a new build control centre will need to identify an overall I&C architecture that will run the automated systems of a plant. There may be multiple design solutions for this I&C architecture, and so it is important that a systematic process is used to identify and select the appropriate solution that supports the end point vision. Both the HSI concept design and the concept of operations can be used as input documents to help define the criteria used to select the appropriate design solution. Alternatively, for design solutions that require integration with existing systems it is important to ensure consistency, as far as is reasonably practical, between the existing and new systems.

To identify available technologies, a benchmark study for similar applications and/or other industries, in which similar technologies have been applied, can be especially effective in the case of new applications. In the case of plant modification, it is typical to choose the same technology as the existing one (i.e. select the same type of analogue switch instead of a digital solution). However, based on a review of operating experience, such as reviewing whether any issue and events are identified in their logs and records, different functions and/or technologies can be followed if, for example, they would help to mitigate known design problems. As an example of this, the design team can review the positive and negative aspects of options available in addressing the I&C component being considered for plant modification. These options may include the following:

— Do nothing and leave the existing component in place;
— Perform a like for like replacement in which the affected I&C is replaced with an identical component;
— Replace with an analogue solution;
— Replace with a digital solution.

The final step of this process is to choose the design solution to be implemented. However, this may not be possible at the early stages of a project. Therefore, a phased approach to the selection and evaluation of technological options that satisfy the end point vision can be implemented at appropriate stages of design maturity. To achieve this, it is often necessary to define and apply selection criteria that can be applied to the different design solutions to help discriminate between them by identifying and comparing their relative pros and cons. This can be done both quantitively, by defining a relative scoring system to different criteria, and qualitatively, by assessing and agreeing on the relative pros and cons of the potential solutions. Typically, a combination of both quantitative and qualitative methods is used, depending on the needs of the project. It is important to ensure that this process is comprehensive and takes account of all relevant aspects of the design and the information in the end point vision, such as the HSI conceptual design and the concept of operations. The following examples can be used to inform the selection criteria:

— Inclusion of adjustments in the existing and/or applied (new) I&C platform, human performance and operation effectiveness (reducing human error), reliability, maintainability and initial and operation costs;
— Consideration of regulatory requirements for the candidate options, as these may require a safety evaluation that does or does not exist, and, in the latter case, this may affect the project's schedule.

Furthermore, it is important to ensure that this process is recorded so that key selection decisions can be reviewed and accessed as the project matures.

The inclusion of any new technology in control rooms can result in positive or negative effects on system performance. It is beneficial for an HFE expert to review a new HSI before it is implemented. If the change has significant impact on human–system performance, it may need a safety evaluation or verification using field tests before implementation.

2.2.2.3. Consideration of emergent technologies

It is prudent to assess potential technology options during the end point vision development. New technologies can bring specific benefits to achieve a design solution but may also come with higher project risk. For example, mobile smart touch screen devices may provide a degree of mobility to plant personnel by enabling them to move around the plant with a portable device. However, if this device introduces new technology, it may require a greater level of testing during design of V&V activities, as it may introduce unknown or unpredictable consequences when implemented. Therefore, when undertaking a high level review of emergent technologies during the development of the end point vision, the overall risk reduction to the project and potential enhancement of the final solution need to be identified and the risks assessed. Furthermore, emergent technology may introduce novel risks to licensing that will also need to be assessed when considering them.

In older plants, hardware and analogue technologies, such as indicators, recorders (with parameter trend implication) and alarm tiles, as well as controllers and switches, are typically used. Some of these interface technologies are augmented with digital technologies (e.g. auto/manual station modules, digital recorders, field equipment).

In new builds, software/digital technologies are typically used, where all fundamental functions (e.g. status/parameter indications, alarms, controllers, switches, field equipment) may use visual display units (VDUs). Therefore, software application technologies take a main role in realizing and representing functions via VDUs.

The change from an analogue technology (e.g. using a continuously visible, spatially dedicated HSI) to a digital technology (e.g. where information is not continuously visible or not all at once) introduces new secondary activities for navigating or accessing the information displayed on the screens. The operator has to investigate the system to find the information rather than it simply being continuously available on an analogue display panel (which requires the operator to remember where the information is and know how to access it). It is one of the comparative drawbacks of digital HSIs compared with conventional HSIs. Ease of use — minimizing the potential for human error while also ensuring that the system is forgiving and tolerant of human error — is a fundamental requirement when using digital HSIs.

2.2.2.4. Consideration of mobile and smart devices

Mobile and smart devices are already being introduced into the nuclear industry and can be expected to become important options for plant modernization as well, especially for new builds. The use of mobile and smart devices in nuclear power plants may reduce the potential for operator error and increase work efficiency and productivity if they are designed and integrated into the wider system effectively. Conversely, they can also increase the potential for human error if they are not specified and designed with the operator in mind. Therefore, it is necessary to understand how a mobile and/or smart device could affect operator and plant performance prior to implementation as well as to consider how mobile devices could affect licensing considerations.

It can be useful to divide the function of mobile and smart devices into devices that are wireless or not. A key consideration for wireless devices, including real time communication (between the signal and the device) functions, is whether the wireless communications negatively affect safety systems through electromagnetic interference. For non-wireless devices a key consideration may be usability, as the risk of electromagnetic interference is not present.

Wireless devices may bring specific benefits to specific situations (e.g. emergency response) and it is important to define whether the design solution needs to satisfy a requirement for such a situation or scenario defined in the end point vision. Additionally, some smart devices may employ advanced software functions such as artificial intelligence, which could support the operator with complex tasks or when under time pressure. However, the potential impact such software could have on safety and wider systems needs to be fully understood. Furthermore, the human error potential associated with smart devices, advanced software and artificial intelligence is less well understood than with conventional HSIs

and commonly used VDUs. Care has to be taken when assessing these potential solutions as they may bring unintended consequences when implemented, such as increasing human error potential.

It can be useful to use the following selection criteria for mobile and smart devices:

— Device characteristics, including functional and physical architecture, technology readiness and regulatory considerations;
— Work domain and operational context of use, including plant states and workplace conditions when these would be used;
— Usability of the HSIs and interactions;
— Integration and harmonization with other HSI systems or devices;
— Human performance, including task accuracy, human errors, workload and situation awareness;
— Computer security aspects;
— Version control and software management.

2.2.2.5. Digital versus analogue technology

Different types of I&C technologies can be considered depending on the necessary safety qualification linked to the information to be monitored and controls to be operated that are critical to safety. The initial end point vision can outline the desired technology to be employed for subsequent analysis and confirmation. Related to the type of I&C, the use of digital I&C is becoming a standard and needs to be considered in comparison to analogue technology. (The latter can be applicable for certain plant conditions such as transients and accidents.)

In any case, the constraints from both HFE and I&C areas and the functions to be fulfilled help to determine the best selection for technology and the final HSI to be implemented.

2.2.2.6. Computer security

Computer security requirements for the system and how the HSI can be the source of vulnerability or the means of defence and recovery have to be considered as described in Ref. [7] and NUREG-0700, (Rev. 2), section 2.9 [8]. From an HF perspective, computer security requirements need to include:

— Barriers to human error such as errors that would result in a security breach;
— The human as an integral element in providing defence in depth through tools that aid recognition of attack and damage assessment;
— Considerations for user identification and authentication (e.g. password locks can prevent inappropriate access but have to be designed in such a manner as to minimize disruption to crucial operations);
— Prevention of data firewalls that would impede optimal system operation (e.g. data that have to be transcribed manually by operators between two different systems).

While protecting against security breaches is important in its own right for nuclear safety, it is important that the I&C engineer balance the above criteria with those pertaining to operability/usability. A highly optimized human–technology system plays a significant role in minimizing nuclear risks.

Therefore, the I&C engineer has to consider the enhanced protections from human error while also considering whether adding in security protection measures will be at the cost of reducing operational reliability. Where conflicts are identified (e.g. where computer security measures significantly slow fault response or prevent it altogether) the safety and security implications have to be considered, documented and resolved by an appropriate advisory group.

It is also important for the I&C engineer to consider the safety classification of security measures. If the failure of a security measure could prevent the I&C system from responding to a fault, then the safety classification of the security measure has to match the safety classification of the I&C system.

2.3. HUMAN FACTORS ENGINEERING PROGRAMME MANAGEMENT

2.3.1. Introduction

HFE programme management is an essential part of any project for ensuring integration of project activities and carrying out HFE when designing and modifying a nuclear power plant. HFE programme management is typically developed in an HFE plan[4], which describes how HFE relates to the project aims and objectives and defines how HFE activities achieve this. An HFE programme is broad and comprehensive and can be applicable to all types of engineering projects for which HSIs are involved across the analysis/design, implementation, operation and decommissioning of a nuclear plant and its equipment.

This section provides practical guidance on HFE programme management, outlining the scope, objectives, activities and key inputs, with special focus in its relation to I&C activities. At the end of this section, some special considerations for an HFE programme management plan are also discussed.

2.3.2. Requirement for HFE programme management

Requirement 32 of SSR-2/1 (Rev. 1) [3] states:

> "**Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.**"

SSG-51 [2] identifies the need for the development of an HFE programme to ensure the systematic consideration of HF throughout the design process. SSG-51 [2] also defines the topics for the expected content of this HFE programme management. HFE activities need to be integrated into the basic stages of an engineering project as illustrated in the example in Fig. 3.

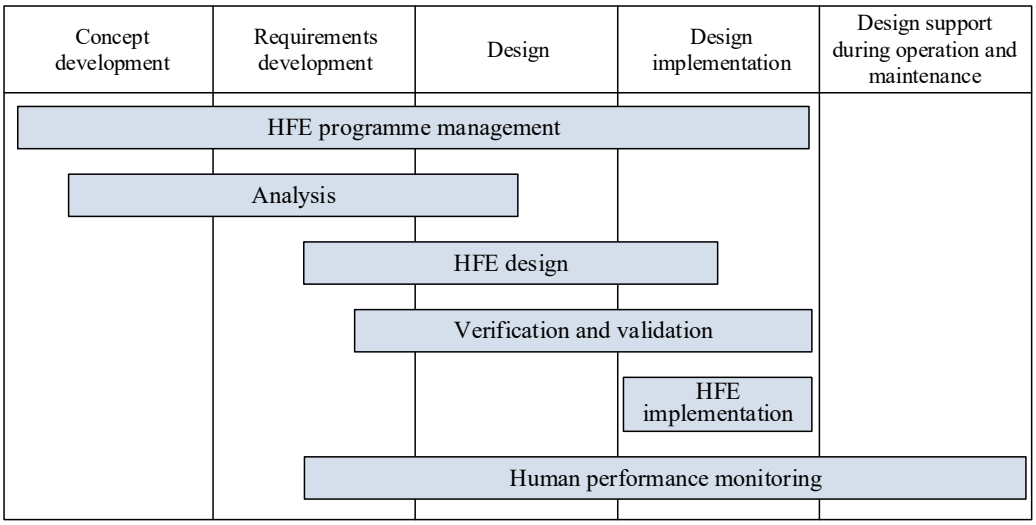


FIG. 3. An example of a generic engineering project, indicating when HFE activities are undertaken. (Reproduced from SSG-51 [2].) HFE — human factors engineering.

[4] This plan can sometimes be referred to as a human factors engineering programme plan, a human factors integration plan or a human factors engineering programme management plan.

In addition to the safety and regulatory requirements, an HFE programme can bring the following benefits to engineering projects:

— *Cost savings:* Early integration of HF analysis, design and V&V activities can reduce costs by ensuring that the design is suitable for the end users, and also by reducing the cost of redesign, implementation, maintenance and training as the design matures and where I&C teams may be involved.
— *Design integration:* The HFE programme management plan:
    - Identifies and integrates HFE activities with the rest of the project's key stakeholders and the necessary interfaces (e.g. with I&C engineering, electrical engineering, civil engineering, V&V teams, regulators);
    - Identifies the key phases of HFE activities throughout the life cycle of the project;
    - Identifies the key inputs and outputs of this process and how they relate to the overall engineering programme.
— *Integration with the end point vision:* The HFE programme outlines the necessary steps required to develop or achieve the planned end point vision by identifying the HFE activities and outputs required throughout the project's life cycle.

Depending on the scale and scope of an engineering project, an HFE programme may require updating as the project matures to ensure that the inputs, activities and outputs are aligned with the rest of the project.

It is important to recognize that developing an HFE programme is a collaborative activity that requires input from many stakeholders. It may be necessary to bring in all of the stakeholders at the beginning of the requirements specification process to support the definition of the HFE programme.

For example, for a control room modification, the requirements development team needs to include engineering, design, operators, HFE, trainers, procedure writers, maintenance, management and any others that would be impacted by the modification. This includes team members to address the following issues:

— Requirement developments that are well thought out with input from all of the stakeholders in the beginning to minimize the requirements related problems as the modification is being developed and implemented;
— Constructability considerations to anticipate installation issues;
— Speedy resolution of issues that may arise during project execution (especially if all engineering teams are aware of one another's responsibilities and what they can all expect from them in terms of analysis and resolution).

This team approach will resolve most of the issues identified above and increase the likelihood that a modification is delivered on time, on budget and, most important, delivers on the expectations of all stakeholders.

For new build plants, the same considerations described for design modifications are applicable (i.e. the supplier needs to have a team approach and there needs to be utility participation). A vendor team with utility participation is also advantageous for modernization projects that are large, complicated and/or high risk to ensure timely utility input and ensure that the requirements and proposed design are fully understood to reduce the likelihood of surprises and increased costs. Regardless of the engineering phase or the composition of the team, HFE input is most effective when the HFE team is considered as part of the design team from the very beginning and not just as an evaluator of a completed design.

2.3.3. HFE programme management plan content

An HFE programme has to meet the needs of the end point vision and the activities, inputs and outputs have to be specific to the project. Consequently, a large new build project would require

an HFE programme that covers the full spectrum of the project from concept to operation and would need to consider how the project will interact with other stakeholders throughout the design life cycle. Alternatively, an engineering project that is upgrading an existing item of equipment would necessarily be smaller in scope and might have fewer interfaces, stakeholders, inputs, activities and outputs.

The HFE programme needs to define, but not be limited to, the items in the following subsections. Detailed guidance for developing an HFE programme can also be found in the Electric Power Research Institute (EPRI) report 3002004310, Human Factors Guidance for Control Room and Digital Human–System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance for Operating Plants and New Builds [9].

2.3.3.1. Objectives

The HFE programme needs to identify the HFE principles and methods that are important to maintain or enhance plant safety. These principles and methods apply to all systems, not only to safety systems. They are important for maintaining or improving operability, reliability and human performance as modernization projects are implemented over the plant's lifetime.

The main objectives of an HFE programme management plan include, but are not limited to, the following activities:

- Defining processes that systematically identify human error potential in the HSI and human performance impacts;
- Defining how the HFE, I&C and other engineering activities and outputs contribute to achieving the end point vision;
- Meeting HFE related safety and performance requirements and expectations;
- Maintaining the plant's HFE design basis;
- Integrating HFE into the project at appropriate activities to allow effective synergies, especially with I&C;
- Ensuring consistency of HSIs;
- Providing HFE input for safety and regulatory evaluations.

2.3.3.2. Scope

The HFE programme can describe the scale and extent of the HFE activities to be undertaken to achieve the end point vision and will define the boundaries, limitations and interaction with the overall project intent and philosophy. The scope of the HFE programme can describe how the level of responsibility and interaction with key stakeholders can change during a project's life cycle. It is particularly relevant for large projects, such as new builds and modernization of control rooms, for which the interaction between the engineering teams and the licensee may evolve over time from analysis, concept design, through V&V and into full operation.

2.3.3.3. Key stakeholders and interfaces

The HFE programme needs to identify the key project stakeholders and their relationship with the HFE and I&C programme of work. These could include, but need not be limited to, the following stakeholders:

- The license holder (this may be a utility or an applicant);
- The relevant regulatory bodies.

— The technical disciplines within the design authority/vendor/supplier, including:
  - Programme engineers and project managers to ensure that programme dependencies/critical path limitations are understood and managed;
  - Bounding representatives of the full population of future users, including operators and maintenance personnel.

Key stakeholders will include those in the following areas:

(a) Nuclear safety
  (i) Probabilistic safety analysis engineers and scientists to provide input to the safety categorization of I&C systems, structures and components, and also inform maintenance, inspection and testing programmes and system response criteria;
  (ii) Safety case authoring team to help establish what level of assurance is required for the I&C system;
  (iii) Internal hazards engineers to provide input to the environmental and fault resilience characteristics of the I&C;
  (iv) External hazards engineers to provide input to the environmental and fault resilience characteristics of the I&C.

(b) Design engineering
  (i) Fault analysis engineers to provide input to the safety categorization and classification of I&C systems, structures and components, including diversity, segregation and redundancy considerations;
  (ii) Process and mechanical engineers to ensure that interfacing I&C and mechanical system requirements are mutually understood and the systems are appropriately integrated;
  (iii) Electrical engineers to ensure that interfacing I&C and electrical system requirements are mutually understood and the systems are appropriately integrated;
  (iv) Civil engineers to ensure that I&C requirements (e.g. cable run space allocation) are appropriately integrated into the design of the civil structures;
  (v) Heating, ventilation and air-conditioning engineers to ensure, for example, that a sufficient cooling margin is provided for the I&C systems;
  (vi) Decommissioning engineers to ensure that, for example, the design of sensors within hazardous environments considers the need for end of life removal and disposal;
  (vii) Information technology engineers to ensure that equipment requirements are effectively integrated into the I&C (e.g. the need for non-safety classified operational/production monitoring);
  (viii) Security engineers to ensure that security requirements are considered within the design of the I&C system and that operational and security requirement conflicts are resolved.

(c) Radiation protection and management
  (i) Radiological protection engineers to ensure that, for example, the design of sensors within hazardous areas specifically considers the magnitude of the hazard and that they are thus designed to minimize necessary human intervention;
  (ii) Radioactive waste management experts to ensure that the I&C specifically considers the need to minimize radioactive waste production, for example, minimizing the number of sensors located in high radiation/contamination areas or designing/procuring components prepared specifically for future decontamination.

HFE programme management needs to clearly define the importance of close coordination between I&C engineering activities and HFE activities (and other design departments such as systems engineering). These two disciplines need to work closely to design effective I&C systems and HSIs that satisfy human performance requirements. HFE programme management also needs to define the key

system interfaces of the engineering project (e.g. the I&C architecture interfacing with the software and displays in a control room).

2.3.3.4. Risk proportionality

The HFE programme needs to establish an HFE graded approach process. The graded approach needs to be flexible enough to ensure that HFE activities are performed and documented commensurate with the size and level of complexity of the risk (see Section 2.3.4.3 for further information on the graded approach).

2.3.3.5. Roles, responsibilities and qualifications

The overall responsibilities for the HFE programme need to be defined. Typically, the primary responsibility for the HFE programme will be with the HF lead. The responsibilities of the other groups supporting this HFE programme also need to be identified and defined. Importantly, the people responsible for HFE need to have the authority to ensure that the HFE activities are given appropriate priority and consideration and that any HFE issues are properly addressed and resolved. The HFE programme needs to include levels of expertise and training for appropriate HFE staff.

2.3.3.6. Activities

The HFE programme needs to identify the HFE related activities required to achieve the end point vision throughout the project's life cycle. These could include the necessary activities required to support the concept analysis, design development, V&V, implementation and operation. The necessary activities, also known as the technical programme, may include, but need not be limited to, the following:

— HFE processes, methods and tools that will be employed throughout the project's life cycle.
— An HFE issues and assumptions register detailing how issues and assumptions will be tracked and treated throughout the project's life cycle.
— Analysis, design and V&V activities required to support the end point vision. These could include design substantiation activities, alignment with design reviews and hold points, design reviews and evaluations.

These activities are detailed in Sections 4, 5 and 7.

2.3.3.7. Inputs and outputs

The HFE programme needs to identify the necessary inputs required to undertake the HFE activities and associated outputs to the rest of the stakeholders as well as HFE related outputs that will be produced throughout the design life cycle.

The inputs may be dependent on the activities of other stakeholders or related to specific project hold points or stage gates. For example, the fidelity of the design will increase as the project matures, and the associated project documentation will require updating throughout this process.

The range and scope of engineering projects can vary greatly depending on the requirements of the project. For example, the inputs into an HFE programme of work for a nuclear power plant may be vastly different from those for decommissioning. The I&C team can help the HFE team to identify the relevant inputs applicable to an HFE programme planning phase. The inputs may include 'external' inputs (i.e. from outside the project such as international standards) as well as 'internal' standards that will be produced by the engineering project from the start and throughout the project's life cycle.

Typical inputs for an HFE programme may include the following:

— End point vision (including the concept of operations and the HSI concept development);
— Engineering philosophy;
— Project plans;
— Mechanical flow/sequence diagrams;
— System design descriptions;
— Logic diagrams, including all the planned system signals and their actuation logic;
— Piping and instrumentation diagrams;
— Regulatory requirements (applicable regulatory requirements are identified as inputs to the HSI design process);
— Operating experience review (OER) of predecessor plants/relevant HSI technology of other industries;
— Power source descriptions.

These documents typically provide the first engineering specification of the plant being built or modernized. They can be used by the HFE team to define and undertake the subsequent activities of the technical programme as described and detailed in Sections 4, 5 and 7. It is important to ensure that the sequence of events is also well defined and planned.

Outputs can include design substantiation reports, compliance matrices, implementation plans, result summary reports, style guides and user population descriptions.

The outputs identified need to align with the maturation of the design. The output of a task analysis, for example, would be produced before a final design substantiation report.

2.3.3.8. Tracking of HFE issues

A tracking system can have multiple functions depending on the need of the project. Typically, for what concerns HFE, projects will need to record the following throughout the design process:

— Issues identified as part of the design process;
— Assumptions used to inform the design reviews;
— Recommendations made to address the HFE issues identified.

A tracking system enables a systematic process for the documentation and tracking of issues, assumptions and recommendations. Ideally, HF issues will be tracked within a project tracking system for all project issues.

HF issues arise for many different reasons from many different project areas and domains. It is useful to outline the criteria for defining HF issues in the HFE programme as well as to define how they can satisfactorily be resolved.

The tracking of HFE issues needs to define management responsibilities and record the following information:

— Issue identification;
— Issue description and prioritization;
— Issue feasibility (for filtering issues that really need attention and to be sent to the recipient);
— Issue recipient evaluation;
— Issue originator disposition;
— Action for addressing the issue (if any);
— Issue verification (for final checking that the issue has been addressed, if necessary).

Tracking ensures that outputs from HFE are traceable and can be verified against the design iterations of the I&C and HSI. The I&C team benefits most from the issues and recommendations that are being actively tracked instead of handing the design team the entire HFE analysis as an output. The HFE issues and recommendations serve to translate findings into actionable tasks for the design phase.

Due to the nature of the design process, it is important to forward recommendations to the I&C team as soon as they are available. The best practice is to maintain this tracking system and to document the implementation of solutions in design or dispositions as they are understood by the I&C team. Generally, dispositions to all recommendations have to be understood and considered acceptable to HFE prior to the implementation of the I&C.

(a) HFE assumptions

Throughout the design process, it may be necessary to make various assumptions about the design and how it operates. For example, it may be necessary to make an assumption about how many operators are required to run the control during normal operations. These assumptions have to be recorded on the tracking system and reviewed and updated at appropriate phases of the project. Other specific topics for which assumptions need to be made include:

— Areas of analysis for which final data were unavailable;
— Operational security practices;
— Interfacing equipment;
— Design basis accidents;
— Conduct of operations in the MCR;
— Examination, maintenance, inspection and testing arrangements.

Where assumptions relating to the I&C have been made, the designer has to capture these assumptions formally for future validation to ensure that the safety case for the I&C system remains valid.

(b) HFE recommendations

Issues identified throughout the project will require recommendations for their resolution.

It is important to be able to communicate to the design team the relative importance of the recommendations being made. Recommendations can be categorized on a prioritization scale commensurate with risk. Below are two examples of prioritization scales:

(1) Criteria based on multiple categories:
   — *Critical recommendations:* Any recommendation that, if not followed, could reasonably lead to unrecoverable errors or mistakes that would have unacceptable nuclear safety, industrial safety, environmental safety, production or equipment impacts resulting in the inability to proceed with the design. These issues need to be resolved prior to implementation.
   — *Important recommendations:* Any recommendation that, if not followed, could reasonably lead to unrecoverable errors or mistakes that would have significant nuclear safety, industrial safety, environmental safety, production or equipment impacts.
   — *Standard recommendations:* Any recommendation that, if not followed, could reasonably lead to task execution failures and significant task execution difficulties that could be reasonably expected to lead users to create shortcuts or workarounds as compensation.
   — *Optional recommendations:* Any recommendation that, if not followed, could reasonably be expected to lead to recoverable errors or some user frustration with the I&C, even after the expected operator adjustment period to new equipment/processes.

— *Enhancement recommendations:* Any recommendation that will improve the proposed design beyond a level that is considered acceptable presently. Failure to implement an enhancement recommendation is more of a lost opportunity than a risk.

(2) Criteria based on two categories:
— *High importance:* Recommendations that are relevant to equipment or to human actions that are important to nuclear safety, claimed in the overall safety case. There may be some instances where the recommendation may be classified as high but is not related to the safety case. These criteria can be defined on a project by project basis.
— *Low importance:* Recommendations that are helpful to the design but not essential to the usability, maintainability and operability of equipment.

In terms of human errors, the HFE and I&C engineers need to consider that there is a generally accepted hierarchy of effectiveness for recommendations:

— *Eliminate the error possibility:* This can include eliminating the task altogether. If the task cannot be eliminated, then designing the system/component/task such that the error cannot be made is the next most effective way to eliminate the risk of error.
— *Design to support error free use:* If the error possibility cannot be eliminated, then the design needs to strongly encourage correct use and/or strongly discourage incorrect use of the equipment.
— *Design for error awareness and recovery:* If the error can be made, then the design has to alert the user immediately of the error and ideally permit error recovery.
— *Administrative barriers:* This can include procedural and training cues as well as the use of human performance tools.

2.3.4. Special considerations for HFE programme management

2.3.4.1. HFE programme management for multi-unit site installations regarding HSI

The benefits of multi-unit sites with several control rooms can include the potential for shared resources, especially personnel resources, across the units. This potential is related to reducing the analysis, design and V&V activities, as well as the training and licensing burden of staff. However, this benefit can be eroded as the design between multiple units diverges. As the design of I&C and HSI systems between units diverges, there is more of a reliance on personnel to adjust their mental model of the I&C system for different units and to interact with equipment that is meant to perform in the same way but may not. On the other hand, if the HSIs are identical (i.e. indistinguishable from one unit to the next), an error may occur in which the operator operates the wrong unit (although this can be easily mitigated using labels, colour and spatial and visual information presentation methods).

There are some unique considerations for multi-unit HFE programmes:

— The HSI itself, particularly in the case of a multi-unit control room, where it is often subject to partial or piecemeal installations as the funding and resources needed for the implementation must be spread across all units.
— The modifications that can span across a longer timeline, which can result in older technology and different software versions installed in the first unit compared to the final unit (which can complicate configuration management).
— Operating experience garnered from the first installation that may affect changes to the subsequent installations.
— Engineering, procurement and construction contracts with suppliers that are often negotiated per single installation, which minimizes the economic risks to the facility owner should the supplier perform poorly. However, negotiating contracts for only one installation in a multi-unit plant can be

detrimental to ensuring that the same HSI technology is used across multiple units, from which a strict HFE perspective needs to be the goal.

To minimize the potential for divergence (i.e. an HSI that looks, feels and functions differently across multiple units), the following activities need to be considered in the HFE programme:

— Tracking the installed differences between units and the rationale for why the differences exist;
— Planning to go back to earlier installations to make changes necessary to minimize differences if a significant impact is determined;
— Performing an error analysis to confirm that the differences do not result in significant undesirable consequences if earlier installations cannot be upgraded to reflect the most recent installation.

2.3.4.2. Modernization programmes planning and migration strategy

Improvements in technology can offer novel I&C solutions. However, the rate of change of new technology can introduce obsolescence risks to the I&C and HSIs. There is also a risk that changes to the I&C can be made in isolation without full consideration of the wider impact on the HSI. To avoid changes made in isolation, an HFE management plan may need to include how obsolescence and change risk are managed.

In addition, when plants are modernized with newer digital systems and their additional capabilities, the plant often does not choose to use these capabilities. This is true even when these additional capabilities could result in enhanced safety and/or improved performance. An HFE management plan can be used to identify the HFE activities required to exploit the benefits of new technology and the capabilities of newer digital systems. It can also help identify HFE activities to be performed so that the design does not create new HF or operability problems.

Typically, when planning for plant modifications, the requirements are developed in isolation by the primary group responsible for the modification. These requirements are used for the design and the implementation work starts on the modification. As modification activities continue, problems can arise with the interface between existing systems and the modification. Before the modification is implemented, HFE experts can assess it to determine the impact on system performance from an HFE perspective. For example, a modification in the control room may change the way the operators interact with the HSI, which may influence how the team works together; it can also affect operator training requirements, operating procedures and maintenance tasks.

The migration strategy identifies the desired sequence (migration path) of the HFE modernization activities. The goal of the migration strategy is to achieve the defined end point vision for the HSIs in the plant through incremental changes. This includes, in addition to the physical changes to the HSIs, changes in functionality, procedures, maintenance and training. The sequence of HFE related modernization activities to be made at each step will be driven largely by the I&C modernization plan. However, there is typically some flexibility in how the HSI modifications can be sequenced.

HFE related activities for modernization projects vary depending on the needs of the project. Some HFE activities may be defined to reach the end point by concentrating the changes in a few large modernization steps. Others may choose to reach the end point by taking a large number of smaller modernization steps. The smaller, more incremental modernization approach is more common since large modernization steps will most likely require the plant to be shut down for extended periods with associated unwanted loss of power production revenue. Smaller steps are more likely to be made within planned outages or with minor increases in the outage time. In either case, it may also be possible to perform some of the modernization activities while the plant is at power. These decisions will impact the migration path.

There are several inputs and considerations involved in the development of a migration path. Some of the important ones include:

— Gathering inputs that will be needed to develop the migration path. These include the end point vision, concepts of operation, HSI design concepts and failure management concepts.
— Applying HFE guidelines or principles that need to be followed in planning and implementing the migration path.
— Planning the migration steps to allow sufficient time and training to ensure that operators and other users become familiar with the changes and comfortable with the new technologies/functionalities as well as to minimize the likelihood of human errors.
— Ensuring the effectiveness of the HSIs produced at the end of each step, since the modifications have to result in an HSI that is acceptable for operation until the next step is taken. This may result in interim, non-ideal designs and hybrid (i.e. analogue/digital combination) interfaces. It is critical to take into account that each interim HSI needs to be designed to be acceptable for operation indefinitely since plant circumstances and priorities could change, resulting in the next modernization projects being delayed or cancelled and requiring operation with the interim HSIs for an indefinite period of time.
— Developing conceptual designs of the individual HSI changes to be made during migration steps.
— Evaluating costs.
— Minimizing project risks.

When the migration path is being determined, the requirements of the plant's procurement process need to be taken into account. It is also important to acknowledge that the design, development, implementation and testing phases of the modification will usually involve iteration due to any HFE issues that are identified along the way.

2.3.4.3. Applying a graded approach to HFE activities

It is often necessary to ensure that the level of HFE effort is commensurate with the risks of an engineering project. To achieve this, it can be useful to employ a graded approach in which HFE in analysis, design and V&V activities can be implemented in a graded manner. A graded approach to HFE can help to ensure that minor, low risk activities receive an appropriate level of HFE attention matched to the scope and potential impact of the engineering project and will aid in ensuring that a commensurate level of HFE effort is applied. Conversely, the graded approach ensures that greater HFE effort and scrutiny are applied to activities that are more complex and higher risk.

This section provides an example of how to define criteria to develop a risk profile for HFE activities. Other criteria may be used depending on the context of the engineering project.

Defining a graded approach for HFE activities can help to develop a better definition of the scope and depth of these activities, ensuring they are commensurate with the risk and complexity of the I&C. It is desirable for the engineering project to define a process and approach that specify the grading criteria to be applied. Additionally, this approach needs to be documented as a standalone process and/or as part of the HFE programme. Determining the grading criteria for the level of HFE effort is best applied during the scoping and concept definition phases of the project to ensure good integration of HF activities in analysis and design.

At a high level, all risks factor into the overall reputational risk of the project owner (e.g. the license holder). Criteria for grading based on the risk and complexity for an engineering project can be based on several factors. Determining the risks has to give nuclear safety high importance. Other significant factors such as production, equipment and other risks are also important.

Determining the risk of an engineering project applies to all phases of the project and the plant's operational life cycle. This risk based approach, which takes complexity into consideration, can be applied comprehensively to all plant systems, from the MCR to in-field I&C not only for nuclear systems, but also for balance of plant systems.

Factors significant for determining risk in a graded approach may include, but need not be limited to, the following:

— *Radiation risk:* Risk associated with the detrimental health effects of exposure to radiation. This can also be defined as nuclear safety risk, which is any risk to the ability to control, cool, protect and contain the fuel. It is based on nuclear system safety significance (safety systems or systems important to safety).
— *Employee safety risk:* Any risk to workers at the plant's facilities, both conventional and radiological, ranging from minor disabilities/exposure limits exceeded to fatalities or permanent disabling injuries/dose limits exceeded. This also generally takes into account the probability ranging from low, where a worker is exposed to a single hazard for routine tasks, to high, in which the worker is exposed to multiple hazards over a variety of non-routine tasks.
— *Production risk:* Any risk to the plant's production ability, including a forced outage or outage extension due to work required to be completed during an outage, resulting in a financial loss consequence to the plant.
— *Equipment risk:* Risk to the plant's facilities or equipment, with financial loss either occurring periodically for a defined period or as a one-time loss.
— *Environment risk:* Any risk to the environment, both conventional and radiological.
— *Security and safeguards risk:* Actions that the plant takes to mitigate the chance that others would intentionally cause harm using the nuclear substances at their facilities.

Regarding complexity, it is generally based on the extent of the change or intricacy of the design. Risk, in the context of complexity, takes into consideration the consequence of errors; systematic, functional or design basis changes; types of equipment; process complexity and design complexity with regard to the changes of components or systems.

Factors significant for determining complexity in a graded approach may include, but are not limited to, the following:

— *High complexity:* Implementing significant changes to multiple systems (e.g. changing from analogue to digital and the overall way to operate), implementing significant designs to new systems (e.g. new MCR, control room modernizations, replacement of full control systems), and systems and components that impact or interact with each other to a significant degree in which evaluations of interactions and impacts are reviewed.
— *Medium complexity:* Implementing significant changes or designs for a single system or a straightforward change/design to multiple systems (e.g. multiple controllers, multiple I&C components for replacement or design).
— *Low complexity:* Straightforward change to a single system (e.g. single controller replacements/designs or simple I&C component replacements/designs, such as hand switches or indication replacements/designs). Routine tasks and changes are simple and are not due to human error.
— *Very low complexity:* Equivalent design (i.e. identical replacement or reverse engineering with an HSI identical to the previous component) projects that only affect alarms on controlling I&C components, no impact on other operating or maintenance procedures, no changes to interfaces other than annunciations.
— *None:* Regardless of risk classifications, there are no foreseeable impacts on human interaction with the system (including human systems) or processes.

Regarding both risk and complexity, it is very difficult to identify all possible risks and the degree of complexity in the early phases of an engineering project as there can be coupling and/or masking effects that are difficult to identify. Therefore, the basis of the graded approach of the HFE programme needs to be reviewed and updated as necessary.

Ideally, in a risk based graded approach taking into account complexity, the HFE effort aligns with the risk and complexity of the design. A simple non-safety class system upgrade may require less formal HF evaluation than a safety class system. Likewise, a partial system upgrade will likely require less HF effort than a new control centre.

3. DESIGN BASIS

3.1. GENERAL

Paragraph 3.11 of SSG-39 [1] states that:

> "The design basis identifies functions, conditions and requirements for the overall I&C and each individual I&C system. This information is then used to categorize the functions and assign them to systems of the appropriate safety class".

Therefore, there is a project need to define the high level requirements that form the design basis of the I&C and HSIs. HF integration with this phase of the project is important to ensure that (a) HFE is appropriately considered at an early phase of the project, and (b) the HFE activities required to support this phase can be identified at an appropriate time. Many countries legislate for compliance with HFE and these requirements have to be identified at this stage.

Two levels of a design basis can be considered as described in SSG-39 [1]. Concerning HFE related I&C requirements:

(1) An overall design basis, specifying an overall I&C architecture and the requirements applicable to this architecture as well as generic requirements applicable to all or particular types of I&C systems (e.g. digital I&C systems or safety related I&C systems) and mobile digital devices;
(2) A design basis for each individual system with more specific requirements only applicable to that system.

3.2. IDENTIFICATION AND DOCUMENTATION OF REQUIREMENTS

Different projects will have different needs for HFE. Some projects may have a heavy reliance on HFE, while others may not. At this stage of the project there is a need to identify whether the project would benefit from the development of high level HFE requirements or if HFE can provide valuable input into the development of the generic high level requirements. The identification of the requirements is undertaken using different information sources, among which are:

— Utility/plant references, where plant design and operation requirements can be identified, including specific user requirements;
— HFE and HSI industry references (standards);
— HSI platform and equipment references (normally provided by industry vendors);
— Regulatory licensing references (where safety and HF requirements can be identified).

The scope of the engineering project (e.g. new build or design modification) can determine the set of relevant requirements, but in all cases, their identification needs to follow a rigorous and systematic approach. As requirements can come from different sources, identification of their origin can be difficult unless they are appropriately tracked. A requirement tracking matrix can be an appropriate way to:

— Document requirements;
— Provide a unique identification;
— Describe the requirement;
— Reference the information sources;
— Describe how the requirement is to be or has been fulfilled;
— Reference the evidence that demonstrates fulfilment.

3.3. HSI FUNCTIONAL REQUIREMENTS

During the design basis phase, a systematic allocation of safety functions to plant structures, systems, components and personnel is required. At this stage of the project, it may be possible to start to define the high level HFE requirements of the project using the safety requirements as a basis.

At the same time, the required I&C systems need to be identified as part of this design process. The I&C systems at this stage will potentially be identified and aligned with the safety functional requirements.

The functions of the I&C equipment need to provide information and control capabilities relevant to the different plant conditions indicated in Section 2.2 and applicable to the engineering project under consideration.

The HSI design needs to contribute to satisfying the defence in depth concept of the nuclear power plant by containing the following elements:

— Prevention of deviations from normal operation;
— Detection and control of failures for facing and mitigating abnormal operation;
— Controlling accidents within the plant operation design basis;
— Controlling consequences of accidents within design extension conditions;
— Mitigating the radiological consequences of accidents.

3.4. HSI SAFETY REQUIREMENTS

The design basis requires that an I&C solution be suitable and meet the needs set out in the end point vision. Typically, I&C systems play important roles for measuring all plant variables relevant for plant operation, and HSI safety requirements have an important function in specifying these roles. It is important to ensure that HFE experts are involved in the process of developing these requirements so that the HFE aspects of the I&C equipment being considered can be appropriately identified.

3.4.1. Codes and standards

The design basis will identify the I&C and HFE standards to which the HSI complies. From this perspective, IAEA guidelines, IEC industry standards or other international standards can be considered. SSG-39 [1] and SSG-51 [2] provide bibliographies of international I&C and HFE standards.

3.4.2. Safety classification

The functional categorization and safety classification of the HSI functions and equipment have to match the categorization and classification of the I&C functions and equipment of which they are a part. The qualification of HSI equipment needs to be planned and conducted in accordance with the safety classification.

From an HFE point of view, the HSI needs to be as consistent as possible throughout the I&C. Based on the complexity of the HSI design and the HFE task, some recommendations on the graded approach to HFE activities undertaken in HSI design could be provided to the target users (e.g. a small replacement on the HSI component may not require a functional analysis).

3.4.3. Safety requirements

To ensure that the safety functional requirements are met, the design has to provide a suitable and adequate HSI. The role of HFE in successfully realizing safety functional requirements in the design cannot be understated.

Safety requirements related to the HSI need to be identified, specified and integrated into the design basis for any engineering project, being based primarily on the regulatory environment of the country where the project is being implemented.

In the case that no safety regulatory requirements are defined, these could be endorsed from other countries considering the country of origin of the vendor or vendors involved in the project.

SSR-2/1 (Rev. 1) [3] considers the following items of relevance:

— Safety in design;
— Fundamental safety functions;
— Radiation protection in design;
— Application of defence in depth.

The IAEA has identified three fundamental safety functions for assuring safety in a nuclear facility (see Refs SSG-39 [1] and SSR-2/1 (Rev. 1) [3]):

(1) Control of reactivity;
(2) Removal of heat from the reactor and from the fuel store;
(3) Confinement of radioactive material, shielding against radiation, control of planned radiation releases, as well as limitation of accidental radioactive releases.

(a) Defence in depth strategy in design

The application of the defence in depth includes several levels of defence that provide barriers to prevent uncontrolled releases as well as a design that contributes to the effectiveness of the barriers. The levels of defence should be as independent from each other as possible.

(b) Application of single failure criterion

The single failure criterion applies to each safety system, to each safety group and to the related HSI systems.

(c) Diversity

In order to avoid common cause failure, diversity measures are often applied. For example, non-computerized backup control means (indicators, push-buttons, alarms, etc.) could be used as backups of computerized workstations, and paper procedures could be used as backup of computerized procedures.

(d) Priority control

One actuator may receive commands from several systems, such as the normal process control system, the reactor protecting system, a diversity actuation system or a manual shutdown system; in this case, a priority logic is needed to ensure that incorrect data from a low safety class cannot inhibit a safety function.

(e) Inhabitability requirement

The inhabitability requirements for control rooms and other locations need to be included in the requirements that I&C and HSI designers put forward to other design disciplines. For example, under radiation resulting from an accident or under fire conditions, how to maintain staff safety and how to plan an evacuation route have to be identified.

In addition, the conditions and procedures for enabling and disabling activity at each location need to be specified, including, for example, switching between control rooms.

3.5. HFE REQUIREMENTS FROM HFE ANALYSES SUPPORTING I&C DESIGN BASIS

Requirements derived from HFE analyses facilitate the documentation and justification for the I&C design basis (SSG-39 [1]). Providing the origin of, and rationale for, every requirement, including HFE requirements, aids in V&V and in the traceability that all design basis requirements have been considered. The following HFE activities are described here in the context of the development of the I&C design basis and are discussed in depth in Section 4.

(a) Operating experience review

The objective of the OER is to focus on the experience in technology, operation and maintenance relevant to the applicable engineering project. This activity is often linked to the development of the end point vision. Examples of information for guiding the OER regarding I&C include:

— The type of components that fail (and their failure modes) and those that are very reliable;
— HSI issues of predecessor plants having a negative impact on human performance;
— HSI technologies to be considered or I&C technologies affecting HSI;
— System design solutions that result in operating problems and guarantee reliable operation.

(b) HFE analysis — Functional analysis and allocation

Identifying safety functions and allocating functions to I&C systems are important activities in developing the I&C design basis. Likewise, for HFE, identifying the role and information needs of the human in achieving system functional goals is also an important analysis activity. The HFE functional analysis and allocation have a detailed link to the planned I&C by providing answers to the question of ‘what’ is to be done/operated and at the same time defining the degree of automation of the I&C. Examples of input to the I&C can be the identification of new functions not considered by the I&C design or the location of I&C components within the design for better functioning or the identification of new I&C components.

(c) HFE analysis — Task analysis

While not all task analyses may be completed at the time the I&C design basis needs to be developed, preliminary task analyses would provide valuable input into general strategies for how tasks may be carried out by key personnel. As in the case of the functional analysis, this analysis has a detailed link to the planned I&C with the tasks to be completed by the crew and with the specific HSI technologies to be used for each of

the tasks. This analysis will answer the questions of how and when the I&C is to be operated. This link can be utilized in both ways, confirming from a task perspective the I&C design or redefining the I&C design.

(d) HFE analysis — Staffing and qualification

A staffing and qualification analysis needs to be carried out to complete the task analysis and identify the specific personnel or crew members that will carry out the tasks and the necessary qualifications for these defined tasks. For the I&C design basis, an understanding of who has the authority and the necessary qualifications to conduct certain tasks and consequently where these users may need access to HSI technologies needs to be considered in the development of the I&C architecture.

(e) HFE analysis — Addressing important human tasks

Prior to performing the HSI design, important human tasks identified in safety analysis reports, diversity and defence in depth analyses, operating experience feedback or any important references are to be analysed in order to minimize human error in tasks important to safety when designing the HSI. In addition, for important human tasks, the design basis has to consider information that the operators are to take into account when performing these tasks. It has to be ensured that this information will be displayed in appropriate locations and will have the performance characteristics necessary to support the operator actions.

3.6. HSI DESIGN PRINCIPLES TO CONSIDER FOR THE I&C DESIGN BASIS

The following section describes two sets of principles that are normally not sufficiently discussed when developing the I&C design basis and, consequently, often do not appear as a consideration in the design of HSIs:

(1) Principles for error prevention, which advocates error-free operation;
(2) Principles for supporting situation awareness and reducing workload.

(a) Principles for error prevention

The HSI to be developed needs to prevent human error under the different conditions planned for its use. Reducing the risk of human error associated with the operation, maintenance, testing and inspection of HSIs typically involves the following activities:

— The broad application of HF principles and guidance to the design and modification of HSIs/I&C systems (for example, using HSI style guidance discussed in the Appendix).
— A targeted HF assessment of risk-significant human actions and the associated HSIs. Risk-significant human actions are those important to nuclear safety, radiation protection or radioactive waste management. They are associated with the achievement of a safety function, for example, ensuring feed to the steam generators in certain accident conditions.

The Appendix provides further guidance on human error prevention principles.

(b) Principles for supporting situation awareness and reducing workload

A nuclear power plant is a complex system consisting of thousands of items of process equipment interacting with and influencing each other in a complicated manner. An operator is a human who interacts with the process system remotely via the HSI. Consequently, it is important that the HSI supports actual awareness of all significant events occurring in the plant.

During education, training and practical work at a nuclear power plant, each operator forms his/her own mental model of the plant, which reflects a nuclear power plant's behaviour patterns, technological and functional relationships between equipment, possible situations and appropriate methods to manage these situations. It is important that the different HSI approaches that can be followed are consistent with the operator's mental model and include the following elements:

— Categorization and grouping of the HSI components (task based display);
— Use of mimic diagrams (process flow chart display);
— Formation and representation of generalized information (function oriented display);
— Representation of overview information (overview display);
— Ecological approach to visualization of information (ecological display);
— Multilayered representation of information (adaptive display).

The HSI needs to be designed to reduce cognitive workload. Both digital and analogue visualization technologies may be used but they will affect the operator's workload in different ways:

— Digital technology has the advantage of centralizing the information in screens, without the need to move or see detailed information in the distance, being at the same time flexible to include more information and change it more easily. The constraint is that not all the information relating to navigation tasks may be available in one view.
— Analogue technology is good at displaying information at a glance, in a spatially continuously visible approach. The information to include normally is increasingly less flexible to modification, consistent with the use of hardwired I&C.

3.7. SPECIAL CONSIDERATIONS FOR CONTROL ROOM AND HSI OPERATION REQUIREMENTS

Control room and HSI operation requirements are normally an input for process engineers and need to include the main features desired for the HSI of a new build or design modification. These HSI requirements can be based on the specific features of the end point vision described in Section 2. As a consequence, the specification of these requirements needs to take account of the following issues:

— The concept of operations and the different locations within the plant (e.g. normal operation from the MCR, local control stations for certain actions, remote shutdown station for cases when the MCR is unavailable);
— The applicable off-plant locations, such as technical support and emergency response centres;
— The functional role of the different locations within the plant, so that one can estimate the needs at each location;
— The operation duty organization, and for each duty, the number of operators at each location;
— The handling of workstation and HSI equipment failure at each location;
— The features of the facilities, considering overall room dimensions where the installation is planned, layout, number and dimensions of panels and consoles, access paths and lighting;
— The features of the I&C to be installed, considering, among others, the number of systems and components within each system, the type of I&C (e.g. analogue, digital), I&C desired performance features, I&C maintainability features, required connections, required power sources, required operating temperature and ventilation;
— The general HSI features to be considered (e.g. planned workstations, screens, layout, staff involved in the operation, type of navigation, planned software);
— Other specific requirements from the utility.

4. HFE ANALYSES OUTPUT SUPPORTING I&C DEVELOPMENT

4.1. INTRODUCTION

The purpose of this section is to guide I&C system engineers in making use of a standardized approach for HFE as part of planning and design. The fundamental role of HFE is to advocate for the human user of the system, provide general and specific guidance to shape the HSI and facilitate evaluation of the I&C system. The HFE analysis process provides necessary outputs that may guide the design process. Five aspects of HFE analyses are reviewed here, including the OER, function analysis, task analysis, staffing requirements and important human actions.

No specific order is recommended, but it should be understood that information from the different analyses may feed into the other analyses. For example, information from the function analysis may help to define the human actions in the task analysis, while the task analysis may help to define the staffing requirements. It is important to develop a plan for carrying out the HFE analyses, including identifying the planned sequence of activities and interactions and dependencies between those activities (see Section 2.3). As information is acquired and developed across the HFE analyses to support the design, the design may be refined, which requires revision of the original analyses. After completing each HFE analysis type identified in this section, where appropriate, a review of the preceding HFE analyses to determine any applicable updates is advisable.

The plan for the HFE analyses is especially important to ensure that the outputs of the analyses synchronize with the I&C activities. The goal of the HFE analyses is to provide outputs that shape and improve the I&C. To do so, information needs to be presented in a timely and useful manner. The methods described in this section can be applied during conceptual design for defining parts of the end point vision, as well as basic HSI design. The only difference is the level of details of the analyses. Less detailed analyses can help create the design concept, while more detailed HFE analyses will refine and optimize it during the design phase.

The outputs from the HFE analyses provide the I&C and the project design team with inputs such as the following:

— Issues and design choices to avoid (based on operating experience);
— HSI design recommendations;
— Interface design changes;
— Interface interaction requirements;
— Changes to interface interactions;
— Potential human error traps present in the design;
— Required changes to mitigate the human errors;
— Additional recommendations, such as for procedure structures and content, and staffing requirements and qualifications.

The design team can incorporate these design outputs into the design in an iterative manner and address them more completely as the design matures. HFE analysis output examples for input into I&C system design may include the following:

— List of expected users;
— List of tasks for each user;
— List of systems interfaced with tasks;
— Expected frequency of use for each user;
— HSI characteristics supporting error prevention in use;

— Optimal function allocation between human and automation;
— Operational issues with similar systems;
— Required staffing levels;
— Required staffing qualifications.

4.1.1. Special considerations for modernization and upgrades

The HFE analyses performed as part of this process will vary depending on the type of project (e.g. new build or modernization of an existing plant system). Where existing functions are replicated in a like for like manner (e.g. an analogue dial is upgraded to a digital dial) there may be little need to perform new analyses. When potentially significant new functionality or modes of interaction are proposed with an I&C modernization programme, it is advisable to perform new HFE analyses to assess the new system. Sometimes, historical HFE data may not exist (e.g. from legacy plants). In these cases, it may be necessary to undertake the required HFE analyses from scratch. Not all aspects of the HFE analyses may be required for modernization activities; these are dependent on the requirements of the project. For example, the introduction of a new turbine control system may benefit from an OER to ensure that existing human errors are mitigated in the new system, but a detailed staffing requirements analysis may not be required, since there are no changes in staffing expected. A graded approach (see Section 2.3.4.3) to HFE can be applicable to modernization activities. Minor HSI changes, such as updating a simple indicator, may not require detailed HFE analysis. However, it is advisable to install the modified I&C equipment in the plant reference simulator for operator training before making changes in an MCR.

4.1.2. Special considerations for decommissioning

Decommissioning is a dynamic environment in which there is a shift in the model of the I&C implementation. Capabilities of the I&C need to be considered regarding system calibration frequency, maintenance and possibility of damage (e.g. to structures and equipment through physical impact during decommissioning activities). During decommissioning, routines are considerably changed, as new work methods and equipment are introduced into areas that may not have been designed for that purpose. This can result in operators having to work with incomplete systems and potentially with altered system functionality. Decommissioning in one area can affect other areas. Practically, this may mean that previously clean areas in which the I&C was operated are now contaminated and have dust particles that have the potential to affect the reliability and operability of the I&C components in these locations as well as to introduce health hazards. An area operability analysis of the impacts of the decommissioning activities in the surrounding area of the I&C is essential to mitigate this.

The practical implication of it is that the I&C engineer needs to consider how the response of the I&C will be affected by changing environmental and/or radiation background levels as waste is transported in pathways potentially near the I&C. The analyses described in this section could help identify relevant changes in the system and ensure that the system design reflects current decommissioning states and associated hazards.

4.1.3. Applicability of HFE analyses to shape the concept of operations

A concept of operations document (see Section 2.2.1.2) can help shape the design, and the HFE analyses can also serve to refine and populate the concept of operations document. A formal concept of operations document may not be required for all design activities, but it is useful to acknowledge the general concept of operations (e.g. a focus on the end user of the system) to ensure that the outputs of the HFE analyses help to optimize the I&C implementation.

4.2. OPERATING EXPERIENCE REVIEW

The OER identifies and evaluates the I&C and identifies existing issues relating to the operation of that system. The OER provides HFE lessons learned from previous experience with related systems. The objective of the OER is to identify negative features that should be mitigated in the new design and also to identify positive features that should be retained.

The OER involves reviewing experience from plants that operate the same or similar systems, I&C components, HSI interfaces, present designs and other designs and solutions to similar problems to learn from general experience. Different types of information sources can be used for the OER. Overall, the intent is to review documentation and survey personnel to obtain operating experience related to existing HSI issues, so they may be addressed in the design. I&C engineers need to be aware of the OER in terms of the I&C technology regarding maintainability, reliability, functionality, capabilities and performance. The OER can identify error traps or even desired features.

It is essential for the I&C engineer to ensure that the OER is executed with sufficient focus on the HFE issues with the HSI in addition to any I&C equipment issues.

Generally, the OER process will consist of the following steps:

— Step 1: Operating experience data collection.
— Step 2: Identification of HFE issues relating to the I&C aspects (e.g. location, indications, controls).
— Step 3: Analysis and evaluation.
— Step 4: OER tracking and conclusion.

There are many different methods to undertake the OER. HFE issues for the OER could be collected from different sources, such as the following:

— Review of operating experience identified in related plants, similar sociotechnical systems and their associated I&C systems and HSIs;
— Review of recognized industry HFE issues that have been published;
— Review of industry and regulatory near miss and event reports related to specific I&C systems;
— Review of operating experience related to the proposed HSI technology;
— Review of important I&C human actions identified in the nuclear plant design.

For I&C systems such as new HSI technologies that do not have much operating experience in nuclear facilities it may be necessary to investigate similar designs in other industries.

Generally, the OER includes database searches, report reviews, HFE issues identified through interviews with plant personnel and observations in the field.

4.2.1. Database reviews

Database reviews can use external incident and operations databases such as those of the IAEA, World Association of Nuclear Operators (WANO), Institute of Nuclear Power Operations (INPO), United States Nuclear Regulatory Commission (US NRC) and/or EPRI, depending on the nature of the I&C project. Fleet OER, such as the Boiling Water Reactor Owners Group (BWROG), the Pressurized Water Reactor Owners Group (PWROG) and utility OER can also be reviewed. When possible, a review of a plant's internal databases, corrective action programme reporting and historical records of human errors in regard to the affected I&C system can help to provide useful information relating to the OER that can directly impact the design of the engineering project. For modernization activities, looking at, for example, in-house historic data can prove especially informative in identifying HFE system performance problems to be mitigated in the new design. It may also be useful to look at academic research literature for similar behavioural or cognitive phenomena that may apply to the particular systems being reviewed.

It is important to ensure that the database review is comprehensive to identify as much OER as possible. The OER activity is focused on HFE, which includes those events containing HSI issues.

4.2.2. Report reviews

Report reviews involve reading a report, possibly an older HFE report or a report not specifically focused on HFE and I&C, for information that has HFE and I&C implications that relate to the I&C project at hand. Relevant plant specific reports and external reports may include the following:

— US NRC generic letters, information notices and other industry reports;
— US NRC operating plant event reports and generic safety issues;
— US NRC licensee event reports;
— INPO plant event reports;
— WANO event reports;
— IAEA operating experience reports/incident reporting system;
— Other industry and regulator references;
— Previous project OERs;
— Accident/incident investigations;
— Design plans and other reports developed during conceptual design;
— Root cause and apparent cause reports.

4.2.3. Interviews with plant personnel

Reviewing operating experience can provide information to the designer about the tasks that the end user is executing on the current or a similar I&C component or system. It can be helpful to observe walkthroughs (i.e. operators operating the equipment or training sessions of existing personnel performing related activities). Conducting OER plant personnel interviews with the end users or knowledgeable trainers can be very useful in helping identify HFE issues, improvements for efficiency, user preferences and best practices for consideration in the design of the new I&C component/system.

Initially, the HSI designer needs to determine who is appropriate to interview. Interviewing plant personnel who are end users of the existing system is useful, but similar system users can also provide excellent insight. Such users may include operations, maintenance personnel or other users, depending on the I&C team. Note that interviews with experienced personnel are not possible for a plant that has not yet been built. In such cases, interviewing personnel at another existing nuclear installation or interviewing personnel well acquainted with similar installations is appropriate.

The designers or system engineers assigned to the project, while likely being excellent sources of information on the project, are generally not suitable for an OER interview except under special circumstances, such as when they have direct hands-on experience with the system being designed and other suitable personnel are not available.

Email questionnaires can provide useful information but can often miss opportunities to investigate specific areas that may not have been anticipated when the questionnaire was created (but may have been identified in a face to face discussion). Email questionnaires need to leave open the possibility of following up to clarify points and investigate a topic in more detail.

Generally, the interviewer notes the job title and years of experience at the relevant job for all participants interviewed. Age, gender, handedness and the presence of visual defects such as colour blindness may also be appropriate to note depending on the nature of the I&C project. The sample of plant personnel needs to be representative of the existing or target population of plant personnel as a whole. Where specific user input is required, it is appropriate to sample a larger proportion of plant personnel, provided they are knowledgeable about the specific work process.

In some contexts, the I&C and HFE design team may wish to accompany plant personnel performing activities in the field. During such walkthroughs, the team would conduct OER interviews and task

debriefs to gain an understanding of the system and allow the user to provide additional information in identifying recommendations that are specific to the component or certain contexts. Additionally, observation of the tasks being performed by the end users provides the HSI design team with the ability to identify issues or workarounds on the component/system to which the user has adapted and which could be improved in the new component/system design.

As an example, observing the potential for migrating from conventional controls to soft controls may be considered. This activity explores behaviours (via simulator walkthroughs, field observations and other knowledge elicitation methods) that are an important part of user training and interaction with the HSI. Often, when migrating from conventional control to soft control, there is a perception that there needs to be a one to one transference such that the soft control ends up looking like the conventional control with very little consideration of how information and control can be integrated better with other functions or task related information. This could potentially eliminate the possibility of improving the HSI. On the other hand, there needs to be consideration of how users interact with the conventional display or control. To an I&C engineer, this may be perceived as a simple, single action when, in fact, it may be more complicated; care needs to be taken that the advantages of conventional controls are not removed or replaced. Conventional tasks include two key advantages shown below, which might be overlooked if not walked through with users of an existing system:

(1) *Landmarking:* Before an operator carries out an action, they may rest their hand on or hover over the control that they intend to use and survey related indications before actuating the control. Such activities may not be possible, for example, with a touch screen that cannot readily distinguish between a hover and a click activation.
(2) *Flagging:* Temporary physical flags (e.g. paper based or magnetic) are sometimes used to identify indications and controls of some importance as operators go through a procedure. Virtual flags may not be considered in the initial I&C specification because they are not a documented requirement of the control boards. To implement a virtual flag requires dedicated development efforts.

Some typical questions for an OER discussion with end users may include the following:

— General:
  - How many years have you been a control room/field operator or maintainer (or other position)?
  - Could you provide a brief description of some of the tasks that you must perform on the system?
  - What do you like about the system/interface that you would not want to lose?
  - What do you not like about the system/interface and what would you like to change?
  - What features would you like to have that are not in the system/interface?

— Operations:
  - Who is responsible for operating the system, interfaces, portions of interfaces?
  - Are there any issues with monitoring system status (e.g. instrumentation accuracy, alarms, displays, location)?
  - Are there any issues with system/interface controls, actuation of controls, displays or troubleshooting faults?
  - Is annunciation adequate for detecting faults and changes in system status?
  - Are there any issues with manual actuation?
  - Have there been any interface or interface interaction issues while working on this system?
  - Do you find you have sufficient time to perform the required actions?
  - Have there been any abnormal or peculiar experiences using the system?

— Maintenance and testing:
  - Is the physical layout of the I&C equipment conducive to performing maintenance tasks?
  - Are there any issues with testing functions (e.g. location of test, who performs it, feedback) during maintenance or field operations?

- Are there any issues with component testing among maintenance staff?
- Are there any issues associated with the maintenance of the system (e.g. frequency, access, isolation) or need for special tools (such as diagnostic computers, consoles or new technologies)?

In some cases, these interview questions may be combined with data gathering for the task analysis. The examples above are simply to provide guidance, and the questions need to be tailored to the specific project. Also, such questions may fail to elicit practice based knowledge, which may not be easy to articulate for many end users. Additional and follow-up questions can help elicit experience from practice in addition to formal knowledge associated with training.

As in all user centred design activities, it is important to gauge user desires versus needs. The OER may reveal specific design ideas by plant personnel that may not be feasible to implement. Plant personnel interviewed for the OER are likely not design experts, and design recommendations, including unsolicited design ideas, have to be separated from actual system performance. For example, if a control room operator provides a suggestion for a specific screen feature, it is important to find out why he or she would like that feature. If the reason is to address a shortcoming in an existing design, it is important to note the design issue. The specific design recommendation provided by the operator is one of many likely solutions for consideration. It is important to recognize that the main focus of the OER process is on identifying HSI issues and that the outputs from this process can be used to inform the design process.

4.2.4. HFE outputs of the operating experience review to I&C

The OER identifies desirable features and HSI issues related to the I&C that need to be addressed in the design. OER results can be screened out to provide a concise list of findings and recommendations (analysed in detail when applicable) and prioritized (according to their relevance to safety, operation and recurrence). This activity is linked to the end point vision, design requirements and other HFE analyses. Overall, the results of the OER can be structured as follows:

— Findings analysis (selecting those applicable to review objectives);
— Findings prioritization;
— Recommendations for HFE, I&C and other engineering disciplines, such as process engineering.

There are similarities to the issue tracking system discussed in Section 2.3.3.8. However, recommendations from the OER are precursors to the design and are only truly issues if error prone features are implemented in the design phase.

4.2.5. Using experimental data

For some novel or first of a kind technologies, there may not be much scientific research underpinning the suitability of the technology. For traditional analogue I&C systems, there is a sizeable body of experimental and experiential data underpinning the use of panel based HSIs. However, a similar body of data may not exist for screen based or hybrid designs (e.g. touch screens) and operational experience from other industries has implicated screen based I&C as a causal factor in incidents.

On this basis, the designer has to be cautious when implementing advanced I&C HSI solutions, where little evidence exists to support the HSI element of the design. It is advisable to perform an early and comprehensive assessment and review of the interface solutions and to build up a body of evidence that the system performs as expected under all normal and fault conditions. For example, it is well known that cliff edge failure of automation can be extremely difficult to recover from where there is little time to respond. Experimental results may conclude that, in cases where little time exists for recovery, the allocation of this function to the operator is not viable given the consequential failures.

4.3. FUNCTION ANALYSIS

The objectives of function analysis are to:

— Define the functions that are necessary for achieving the plant's goals (e.g. generate electricity and assure plant safety).
— Allocate the previously identified functions to the human, to the machine, or both, based on what each can do better. As a consequence, the identified functions will not differentiate those functions that are manual or automatic at the beginning of the process. Instead, this differentiation will be achieved at the end of the function allocation process.

A function analysis is not limited to overall plant functions and may also be applied to lower level goals at the system or component levels. A function analysis consists of two main steps:

(1) The function requirements analysis (FRA) process;
(2) The function allocation process.

An FRA identifies and determines those functions the system must perform with and without human operators. An FRA can be developed for a new design based on a hierarchical decomposition, where plant goals are decomposed into high level plant functions and into lower level details such as system and component functions. For design modifications, the scope of this analysis is typically interested in the functions that are subject to change, if any. Existing plants may traditionally not have been licensed with an FRA; consequently, a modified system may still necessitate a complete FRA.

4.3.1. Function requirements analysis method

The purpose of an FRA is to analyse and designate the essential plant functions systematically.

Typically, as a starting point, the FRA uses the system design descriptions of plant systems, where the system functions are described and where system components and parameters are identified. Other I&C technical information such as logic diagrams, power sources and piping and instrumentation diagrams can be used.

The FRA aims to bring together the I&C with HFE analyses and it plays an important role in integrating I&C with HFE.

When undertaking an FRA, it is important to identify the system functions. Each function can then be further subdivided into processes where plant system components are involved in a specific function. The analysis will require identifying function/process requirements necessary to achieve the functions in terms of parameters (i.e. function need/evolution of the process), controls and support requirements.

The functions to be analysed from a plant perspective can be substantial and a screening process can be developed for analysing those functions that are more representative for plant operations, related or otherwise grouped. The FRA results may vary depending on different plant operating modes.

For example, the plant protection systems might consist of of the following functions:

— Reactor and fuel protection;
— Equipment protection;
— Fire protection;
— Safety actuation;
— Radiation monitoring;
— Seismic monitoring.

These functions would, in a typical nuclear power plant, be handled by separate systems (although these systems may not necessarily be diverse). The I&C engineers would determine the best hardware and

TABLE 1. EXAMPLE FUNCTION REQUIREMENTS WORKSHEET

No.	Function requirement	Identification of control functions				Performance characteristics of control functions						
		Control requirement	Control behaviour	Control variable	Verification variable	Workload	Time limitation	Accuracy	Repeatability	Complexity	Estimation method	Effect by failure

software systems for these functions. Where such systems involve interfaces with human operators, the HF engineers would provide input on the optimal HSI to support these functions.

Table 1 presents an example FRA worksheet. This table may be modified to meet project needs but provides a good starting point regarding the types of considerations for FRA and the type of impact it might have on HSI performance.

4.3.2. Allocation of functions to human and/or machine method

After the FRA has been completed, the next step of the functional analysis is the function allocation. The previously identified functions need to be further analysed in terms of how the activities will be carried out. The purpose of function allocation is to identify which functions should be automated and which ones should be performed manually. Automation may take two forms:

(1) Control automation, which involves systems performing tasks automatically;
(2) Information automation, which involves systems gathering information automatically.

Plant functions have to be monitored, understood, planned and allocated, which mirror the roles of control and information automation. Each function has to be analysed to determine the following questions:

— If automation is desirable for performing the function;
— If automation is best for performing the function;
— If humans are desirable for performing the function;
— If humans are best for performing the function;
— If automation and humans should share the activity.

Humans and machines have specific capabilities and limitations that are useful to know when allocating functions. A good source for this information can be found in Ref. [10]. It is important to note that while human capabilities and limitations have largely remained unchanged, the capabilities and limitations of machines are constantly improving and changing. Recognizing this fact is important to ensure that up to date information is applied to the design. Generally, humans are not as good as machines at repetitive or monotonous tasks such as continuous monitoring; however, it is important not to exclude the operator from the system monitoring activities so that they can maintain an up to date awareness of the

system status. Humans tend to be better than automation at decision making given adequate information and recovery activities in the face of plant upsets.

Automation is not, in a general sense, all or nothing, and function allocation will also determine different contexts and what level of automation might be appropriate for each context. Some technologies allow a switch between different levels of autonomy as needed. For example, the plant automation system may need to provide additional visual information during tasks that require a high degree of monitoring by the operators.

Functions are increasingly shared between humans and automation, and the extent and the characteristics of this sharing of functions needs to be better defined and needs also to take into account that there can be a spectrum for the extent of sharing. The level of automation may not be fixed and may adapt to fit certain contexts. Also, in different plant states the same function may have a different level of automation.

The following items, adapted and expanded from EPRI TR-1011851, Guidance for the Design and Use of Automation in Nuclear Power Plants [11], need to be considered as part of function allocation:

— *Digital versus analogue hardware considerations for relevant systems:* Determine if the system should be digital or analogue and consider how this impacts manual operations performance and opportunities for automation.
— *Essential automation checklist:* Determine which functions need to be automated. Such functions may feature high human error rates and high consequences for errors. Such functions may have the following characteristics:
    - Manual performance of the function raises health or safety concerns.
    - The function has to be performed very rapidly.
    - The function requires precision beyond human capabilities.
    - The function requires human reliability greater than is available. Human reliability may be determined by using a human reliability analysis (HRA) method.
— *Desirable automation checklist:* Determine which functions would benefit from being automated. While humans may perform these tasks, they do not do them well and they may be error prone, even if the errors are not of serious consequence. Such functions may have the following characteristics:
    - The function is complex and easier for computers to perform;
    - The function requires many repetitive actions that may be fatiguing or boring to operators;
    - The function creates high cognitive workload;
    - The function creates long periods of boredom;
    - The function creates high physical workload or fatigue;
    - The function interferes with the performance of another (manual) function if not automated;
    - The function could be performed more efficiently (e.g. quicker) if automated;
    - The function could reduce staffing levels if automated.
— *Essential human automation checklist:* Determine which functions need to be performed manually. In such cases, human reliability exceeds automation reliability. Such functions may have the following characteristics:
    - The function is a core human responsibility (e.g. communicating to field workers);
    - Automatic response is difficult (e.g. the function is challenging to model in control logic);
    - Personnel must remain ‘in the loop’ (e.g. a human operator needs to take over control or a human operator needs to maintain vigilance and situation awareness);
    - Personnel must retain skills that would be lost if the task were automated.

4.3.3. Output of the function analysis to I&C

The function analysis output will recommend a list of automated functions, a list of manual functions and a list of functions with auto/manual combination. It may also specify what information the human operator needs for assessing the status of the different functions.

An issue tracking system (see Section 2.3.3.8) needs to be considered in the planning phase to ensure that the findings of this analysis are taken into account and documented as appropriate. In some cases, changes to the system to address the outputs from functional analysis may require engagement with a formal project process, such as an engineering change request. In other cases, when the analysis is performed early in the design phase, the information from the function analysis influences the specification before it is finalized. Examples of engineering change requests include:

— Identification of new functions not initially planned;
— Change of the location of the I&C component within the plant for assuring best function performance;
— Proposals for changing the type of I&C component for manual versus automatic actions.

4.4. TASK ANALYSIS

4.4.1. Basic approach

Task analysis is a methodology used by HF experts to provide a logical description of human-system interactions that occur while users take actions to achieve a goal or objective in a given environment. The analysis also explores how they perform their tasks and reach their planned goals.

Task analysis can provide the I&C engineer with useful design input to determine the following:

— The points of interaction between the human and the system;
— The sequence of actions performed in carrying out a task;
— Those tasks that may be error prone along with suggested design improvements;
— The potential for human error;
— Information needs during particular tasks.

General HFE practice places task analysis between the completion of HFE planning and the beginning of HSI design. However, based on the maturity level of design information available at the early design phase, iterative reviews of task analysis results are advisable for the subsequent HFE process. In particular, the HFE V&V phase and design implementation phase can provide significant feedback regarding human performance issues. The task analysis needs to be reviewed and revised if necessary, based on evaluation of HFE V&V and design implementation results.

The task analysis data are a principle input to the task verification process, whereby the I&C is verified against the requirements of the user. For example, if the operator of a system needs to have access to specific information screens or particular controls, the task analysis will identify this requirement to the I&C engineer to ensure that these features of the system are available during that task. Task analysis data can also be used to underpin the quantification of human errors for use within the HRA.

The task analysis needs to be appropriate to the I&C project and often has to represent the full range of plant modes, including startup, normal operations, low power and shutdown conditions, transient conditions, abnormal conditions, emergency conditions and severe accident conditions.

A task analysis may break down system functions into constituent human tasks and subtasks, whereby a task represents a set of actions towards a particular goal. It is possible to break down tasks into lower and lower levels of subtasks, if required. To prevent needless detail and decomposition, screening criteria can be established to select the tasks for analysis, and ‘stop rules’ are set to determine how far into

a task decomposition it is necessary to go. Tasks necessary for the analysis include important tasks that may affect plant operation, performance and safety.

The FRA specifies manual/automatic allocations of major plant functions, which in turn support safety and power generation goals. The task analysis also includes manual tasks, which are allocated to humans, as well as monitoring or oversight tasks, which are allocated to automation. As a result, task analysis typically identifies the relationship among tasks (i.e. tasks carried out in sequence or in parallel or that are conditional to other tasks), time estimations required to complete the tasks, number of people and specific performers for each task and knowledge and abilities required to perform the tasks.

The general process of task analysis consists of the following steps:

— Step 1: Specifying the scope (i.e. tasks to be considered).
— Step 2: Establishing the screening methodologies and criteria.
— Step 3: Identifying tasks to be analysed.
— Step 4: Selecting applicable task analysis methodologies and conducting the analysis.

The scope varies in accordance with the project. Once the tasks that will need to be analysed are identified, task analysis typically begins with a high level review, such as a breakdown of key functions into tasks. These tasks essentially identify what the operators are required to do. The task analysis can adopt various methods to describe greater levels of task detail such as operation sequence/timeline analysis, cognitive work analysis or hierarchical task analysis to identify which HSI inventories and task support functions, plant diagnoses and workplaces are required and what workload, situation awareness and other performance shaping factors look like. Annex I provides more information on HSI induced cognitive error analysis.

In the case of an upgraded plant, fit and gap analyses are typically performed to identify the new scope and objectives to be analysed. Scenarios and assessment baselines can be identified at an early phase of design. Operating procedures (if available) may guide much of the task analysis activities because procedures represent a formalized task list for operations and are, essentially, a type of documented task analysis.

In the case of a new plant, the analysis can start with relatively incomplete information and may need to make specific assumptions about the HSI. Scenarios may be obtained from preliminary plant design information. An iterative approach task analysis may be required when design information is updated, assumptions are changed or different stages of design are achieved.

Subsequent analyses and HSI design will use the task analysis results and assumptions for further investigations and realization of the design (i.e. establish the design specifications). For example, the task analysis provides the location where tasks are being performed with consideration of the work environment and potential hazards. A suitability analysis to select HSI design options can be implemented to determine which HSI design options are preferred prior to finalizing the design.

A review of implementation issues can take many forms depending on the nature of the project and how it is being implemented. An original task analysis of the tasks being performed during the implementation phases or an edited/adjusted version of a task analysis performed as part of an already completed HFE review are common methods of approaching a review of implementation issues.

Implementation issues can be reviewed considering the following specific aspects:

— Whether the analyst believes there is a chance that installation activities will distract or disrupt operational or maintenance activities in a manner that creates or increases unacceptable error possibilities;
— Whether unique operational or maintenance activities exist during the implementation phase that were not reviewed during the task analysis portion of the HFE review;
— Whether the analyst believes that the expected implementation strategy might increase the possibility of unacceptable human errors.

It is useful to undertake an implementation review prior to the end of detailed design. This ensures that HFE recommendations can be understood prior to (and addressed during) implementation.

4.4.2. Area operability and impact analysis

An operability and impact analysis is a type of task analysis used to assess the impact on human performance of HSIs in the area where a system is being implemented. For new designs, the purpose of the analysis is to determine the accessibility of equipment and impacts of co-located systems on the users of those systems. During design modifications and upgrades, the area operability and impact analysis can consider the following changes:

— Changes to the accessibility of HSIs on nearby or connected structures, systems and components such as displays, controls, maintenance points and testing points;
— Changes in usability of nearby HSIs due to changes in ambient noise, lighting, vibration, heat, etc.;
— Changes to the ability to move people and equipment in the area.

An area operability and impact analysis is required to address the above issues relative to normal operational activities, abnormal operations, maintenance activities, testing activities and emergency situations. It takes into consideration the location where the equipment is being installed and the surrounding location that could potentially be impacted with the new component or system installation. It also determines if the equipment impacts the area in which it will be installed (i.e. does it obstruct traffic flow; affect maintenance or operation on surrounding equipment; add or increase environment issues such as heat, noise or space constraints?). This analysis involves the review of floor maps of the area around the piece(s) of equipment being installed. Access to other pieces of equipment is noted, including swing arcs of access doors, standing locations of users or maintainers and main paths of travel for equipment and personnel through the area. The nature of the I&C may also require the review of a relief drawing to note if the piece(s) of equipment being installed will affect lighting in the area or lines of sight to nearby displays.

4.4.3. Outputs of task analysis to I&C

Task analysis outputs provide the designer with key information about user tasks that drive interface design and usability and the feasibility of performing tasks with the HSI design. It tells the designer what tasks the operator performs (and how they are performed) and what support (e.g. operator aids, alarms, indicators or additional staff) the operator needs to complete those tasks. Overall, it gives recommendations that drive the initial design or subsequent changes or modifications to the I&C and how the I&C is used.

As an output of the analysis, the I&C engineer receives the following:

— Lists of scenarios with associated tasks (if they are achievable in parallel or if more staff are required);
— Inventory of alarms, controls, indications and other interface components required;
— Scenario/task timing constraints.

4.5. STAFFING AND QUALIFICATION ANALYSIS

The main objective of staffing and qualification analysis is to determine who will perform the tasks identified for plant operation in the task analysis and the qualifications required for accomplishing these tasks. Other inputs that could be required are the concept of operations (see Section 2.2.1.2), regulatory requirements and operating experience applicable to this activity.

As described in SSG-51 [2], the staff covered by this analysis can include operations personnel (i.e. MCR personnel and local or field operators), service support teams and emergency preparedness and response teams. Typically, a three-step approach could be considered in a staffing and qualification analysis process:

— Step 1: Determination of the initial staffing and qualifications;
— Step 2: Revision of the initial staffing and qualifications after completion of the detailed activities coming from HFE;
— Step 3: Final staffing and qualification recommendations after completion of the HFE programme.

4.5.1. Initial staffing and qualification levels

Initial staffing levels can be established based on existing experience with previous or similar plant designs, initial analyses and government regulations.

As an example, traditionally in MCRs the shifts are composed of a reactor operator (in charge of the plant's primary side), a turbine operator (in charge of the plant's secondary side), a shift supervisor (managing and supervising both operators and shift manger) and a shift manager (responsible for the shift and rest of the activities outside the control room). Many plants also include a shift technical advisor (supporting reactor operators without controlling the plant). Sometimes the naming and responsibilities may vary depending on the type of plant or geographical region.

The level of qualifications among the crew members may vary depending on the plant design and national qualification requirements. The license to operate the plant resides with the reactor operators (also known as reactor operator license and senior reactor operator license). In some designs a turbine operator license also exists.

The qualifications can be established following several possible methods, including the following:

— Qualifications based on operating experience of previous designs where training programmes already exist and can be mapped to the specific tasks to be completed;
— Qualifications to follow a catalogue of knowledge and abilities that are available for different types of reactors and mapped for the task under the scope of this activity;
— Qualifications based on regulatory requirements;
— Training standardized by a qualifications board, such as INPO;
— Qualifications based on a particular vendor's training programme.

4.5.2. Revision of the staffing and qualification levels

The staffing analysis, like most HFE analyses, is iterative. As additional information is gathered on the design and tasks, staffing and qualifications may be revised. The crew members who will perform the tasks defined in the task analysis (i.e. those tasks that are not automated) need to be identified. The typical approach for performing the staffing analysis follows the output of the task analysis. Depending on the method followed, task analysis outputs can provide:

The tasks to be completed for fulfilling system functions (normally assigned to one operator);

The tasks for carrying out plant scenarios covering normal, abnormal, emergency and accident conditions and encompassing different plant modes;

The tasks of these plant scenarios that affect more than one person, because of the purposeful redundancy in roles and responsibilities, connectedness of different tasks to shared systems and interdependencies caused by sequencing of tasks.

The typical approach is to assign tasks to those operators already identified in the initial staffing levels to systems.

The examples below could modify the staffing and qualification levels:

— An HSI design issue with the use of unplanned technology or new design solutions that can affect the defined qualifications;
— V&V results that recommend increasing knowledge and abilities when executing a specific task.

Revisions are finalized prior to implementation. Multiple iterations may be possible throughout the design life cycle of the plant.

4.5.3. Output of the staffing and qualification analysis to I&C

The staffing and qualification analysis output results could confirm the I&C overall design or provide design modification recommendations from an HF perspective. They may also identify HFE insights that impact the I&C:

— Identification of tasks that may require extra operators (such as relocation of controls requiring an increase of staff for interface use or multiple control stations requiring separate operators);
— New functions not initially planned that require operator monitoring or actions;
— Identification of tasks removed from an existing system (e.g. through increased automation), resulting in a significant decrease in the amount of workload among existing staff;
— Changes in tasks on an existing system due to new I&C, resulting in changes to required staff qualifications (e.g. digitizing the HSI, requiring specific computer system training);
— Changes in the placement of the I&C components within the plant that change the location of operator activities.

4.6. TREATMENT OF IMPORTANT HUMAN TASKS

Throughout the HFE analysis phase, human activities or tasks are identified that could impact successful operation. Every human task identified in the task analysis has, for example, the potential for error that could undermine the safety of the processes.

Those human tasks that impact I&C and plant safety are considered important human tasks. Important human tasks need to be identified to ensure that the planned HSI design will minimize the likelihood of human error or mitigate the effects of any error that occurs. Important human tasks can be determined from the probabilistic safety assessment and accompanying HRA[5] and from other aspects of the HFE analyses such as the task analysis or staffing and qualification analysis. Risk-significant human tasks are those that potentially increase the probability of core damage. In HRA, risk-significant human tasks are typically associated with plant conditions or scenarios where manual operator tasks are necessary for correct alignment of plant components, and an operator error can challenge critical safety functions at the plant. Examples include general design basis accidents, where manual tasks can be necessary.

In general, risk-significant human tasks are associated with hardware systems that affect the safety of the plant. In HRA, human failure events are defined as human tasks that contribute to the failure of hardware systems or components at the plant. In the absence of a formal HRA, which may not be modelled for all

[5] IAEA Safety Standards Series No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [12] provides a structured approach to human reliability analysis for the identification of different types of human interaction. The human reliability analysis includes human errors made before the occurrence of the initiating event that have the potential to lead to the failure or unavailability of safety related equipment or systems (usually referred to as Type A human interactions), the potential human errors that could lead to an initiating event (Type B human interactions) and the critical tasks that will need to be carried out by plant operators after the occurrence of an initiating event (Type C human interactions).

systems, an understanding of crucial plant functions and the task analysis linking human activities to particular systems provides a roadmap for important human tasks. If the system is important to the safety of the plant and the human interfaces with that system, the human tasks are likely significant for the overall risk of the plant.

When upgrading a plant's I&C, there is an opportunity to increase or decrease the likelihood of human error. The following cases warrant a fresh review of important human tasks (see NUREG-1764 (Rev. 1) [13]):

— Temporary or permanent plant changes, including I&C upgrades;
— Temporary or permanent procedure changes;
— Temporary or permanent training or qualification changes;
— Any other changes in the human tasks associated with the I&C (e.g. changes in environment or teamwork composition).

4.6.1. Analysis of important human tasks

Once the important human tasks are identified, the associated I&C and HSI components involved with these tasks need to be identified with the help of the task analysis previously performed. The planned I&C and HSI components need to be analysed for how the I&C equipment being placed or replaced affects the ability to perform important human tasks. Key questions to be answered include:

— Can the I&C affect an abnormal incident response or design basis accident response?
— Can the I&C affect the sequence of the response required to be performed for the abnormal incident/ design basis accident?
— Can the I&C affect the human response necessary to execute the tasks?

The system design has to take the following considerations into account:

— Ensuring that personnel can detect and recover from any errors;
— Determining if the I&C equipment affects the staffing levels needed to execute the desired task and, therefore, impact minimum shift complement;
— Calculating the number of steps and associated time required to complete particular tasks;
— Determining the possibility of introducing new types of human error with new I&Cs or HSIs.

It may be desirable to quantify the likelihood of human errors. Most HRA methods allow the possibility of quantifying the human error probability, even without a formal plant-wide HRA. Such screening analyses on particular human tasks may consider performance shaping factors that serve to increase or decrease the probability of human error. These performance shaping factors (e.g. level of training, quality of procedures, environmental factors, task complexity or quality of the HSI) provide keys to the drivers on performance and specific ways to improve the outcomes of human tasks. HRA quantification can help to prioritize which HFE issues can impact plant safety. It may be helpful to assign acceptance criteria for human error probabilities.

4.6.2. Outputs of important human tasks to I&C

The output of the HFE analysis on important human tasks is a list of the identified important human tasks with the proposed HSI solution for addressing potential human errors. Examples of this would be replacement of an existing I&C component with a different component that requires fewer or simpler task steps to complete the required action.

Although nuclear power plants operate with very high rates of human reliability, it is never possible to completely prevent human errors under all circumstances. Therefore, the plant design and the I&C need to ensure plant safety by minimizing the impact of human errors on important activities and functions. Furthermore, the I&C needs to provide mechanisms such as safety systems to recover from or prevent human errors.

5. HSI DESIGN PROCESS

5.1. CONTEXT

SSG-39 [1] and SSG-51 [2] provide HSI design guidelines that should be considered. This section focuses on the HSI design process and its interactions with I&C architectural design, process design, plant systems design, procedures design and training programme development, as possible conflicts affecting HSI design need to be jointly resolved. For example, the I&C architecture must provide multiple and independent levels of defence in depth. However, having an independent and diverse HSI for each level of defence in depth might not be a good solution from an HFE standpoint. Additionally, the design process can vary between different organizations and Member States.

5.2. OVERALL PROCESS

The goal of the HSI design process is to specify each HSI function and each HSI system. The HSI design needs to take into account the specific roles, functions and capabilities as specified by the I&C architecture. The HSI systems need also to meet the specific requirements from the other design activities such that their integration into the plant accomplishes safety and operational goals.

To accomplish the design process successfully, a systematic approach needs to be applied. Figure 4 depicts a typical but simplified version of an HSI design process with examples that translate requirements into HSI design elements (e.g. alarms and the information display to be used) and the interfaces (i.e. operational and physical) that are combined in the final integrated HSI. In reality, the design process can have multiple iterations at the various stages described in Fig. 4.

As stated in Section 2, the conceptual HSI design and the concept of operations are developed for the end point vision. The specific requirements to be applied first need to be identified. Requirements and design inputs, such as lists of controls and monitoring information to be provided in the MCR, need to take account of HF analysis results and recommendations (see Section 4). The I&C and the HFE teams need to conduct cross reviews of individual requirements from the other disciplines, then generate harmonized requirements/conclusions for common technical areas, such as the levels of automation. The following subsections specify what activities need to be incorporated into each HSI design activity after receiving requirements and inputs as specified in Sections 3 and 4. As some HSIs could be relatively complex, particularly in the case of digital HSIs, using a step by step approach to HSI specification is advisable. The three steps described in Sections 5.4, 5.5 and 5.6 include an HSI overall specification step, an allocation step and an HSI detailed specification step. However, before HSI specification can begin, the design team needs to harmonize requirements from various sources, as described in Section 5.3.

5.3. SPECIFICATION OF HARMONIZED DESIGN REQUIREMENTS FOR EACH HSI

5.3.1. Purpose

The HSI design process typically starts with the specification of detailed design requirements for each individual HSI, based on various sources (end point vision, regulatory documents, standards, etc.) as refined in the HSI design basis development and HF analysis, respectively. However, potential conflicts between design basis requirements from different stakeholders or between HSI design basis requirements and HFE recommendations need to be resolved. In the case of a new plant and or a large modernization project, HSI design often needs to prioritize, harmonize and negotiate various requirements to meet plant safety and operational goals and the overall end point vision. At the same time, the design has to consider the capabilities and limitations of available I&C platforms and equipment.

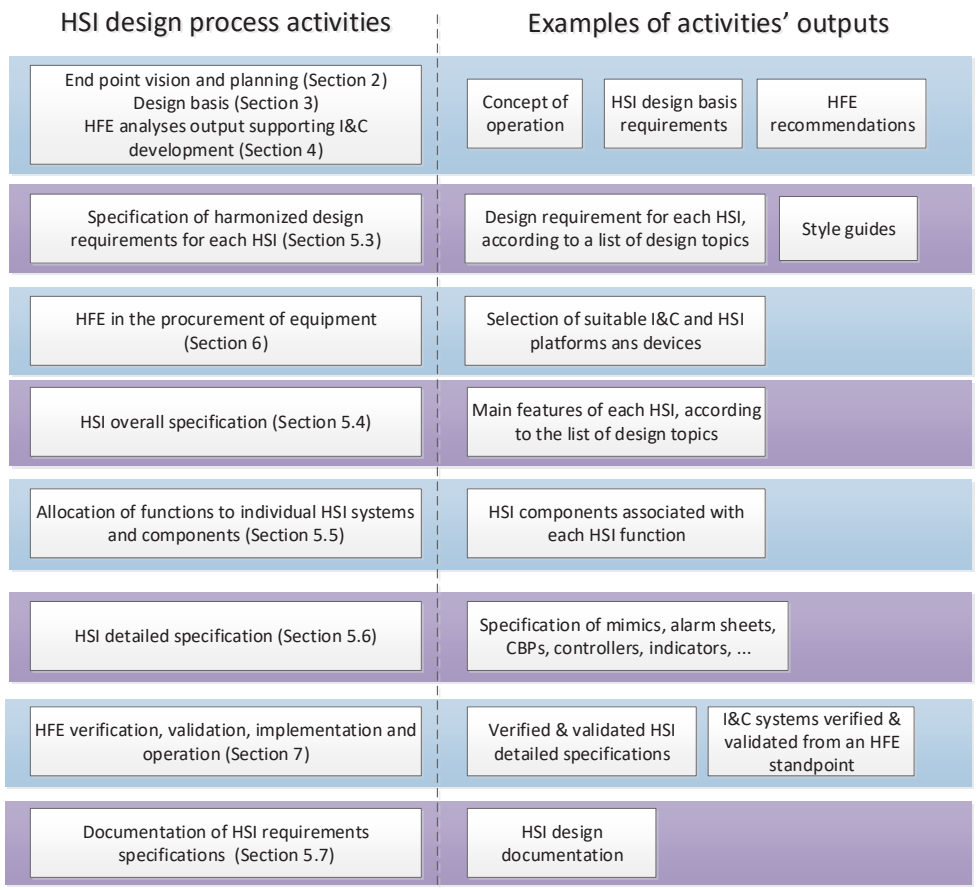


FIG. 4. Example of a design elaboration process. CBP — computer based procedure; HFE — human factors engineering; HSI — human-system interface; I&C — instrumentation and control.

The specification of the detailed HSI requirements may also need to consider how particular requirements may impact the overall I&C performance. In a small modification project, the scope of design and specific requirements from various stakeholders are typically more limited. Subsequently, this activity might not be necessary.

Also, some HSI design basis requirements or HFE recommendations may be too prescriptive, ambiguous or imprecise, and thus might need to be reinterpreted.

5.3.2. Methodology

To facilitate the identification of conflicts, HSI design basis requirements and HFE recommendations may be grouped into design topics (e.g. 'alarm display' or 'information display'), as conflicts are more likely to affect requirements within the same topic. If contradictions are detected, conflict resolution may be achieved in the following ways:

— Through joint work involving the multiple disciplines and stakeholders concerned (including I&C) to verify key assumptions and requirements, to gather new ideas and to determine the core design elements that collectively achieve the associated requirements or to prioritize requirements if they cannot be harmonized;
— By use of mock-ups and/or prototypes to identify and/or help to find appropriate trade-offs.

Some HSI design basis requirements or HFE recommendations are high level and merely specify the overall objectives. These often need to be refined into more operable, detailed HSI requirements, based on specific solution principles.

The specification of the detailed HSI requirements may necessitate a revision of the end point vision (see Section 2) of the HSI design basis requirements (see Section 3) and of the HFE recommendations (see Section 4). Revision of the end point vision and the HSI design basis requirements may require end user engagement.

The detailed HSI requirements are used by the I&C team to implement the specific HSIs, which may result in a documented design specification. Additionally, an HSI style guide may be developed to provide overarching design guidance (see the Appendix). An HSI style guide provides a bridge between design topics and ensures consistency across HSI applications. While the detailed HSI requirements specification is a specific instantiation of a design concept, a style guide is a general document on the 'look and feel' of the HSI that shapes the specification. Development of the style guide and the user population design ranges needed to inform the style guide is described further in the Appendix.

5.4. HSI OVERALL SPECIFICATION

5.4.1. Purpose

The purpose of an HSI overall specification is to identify the main features of the HSIs concerned. In the case of a digital HSI, this could mean the specification of generic principles, functions and capabilities for general services such as alarm management, display navigation, information display, and the like. In the case of an analogue HSI, this could mean shape, size, layout principles, and so on.

5.4.2. Methodology

The first step is to determine whether the technical features of the available I&C platforms and equipment could meet the specified, detailed HSI requirements. If none are found through a documentation review or a review of similar industry applications, prototype studies may help decision makers identify which particular platforms or equipment could meet requirements. The design elements and style guide may be amended if no product can be aligned with the detailed HSI requirements.

The second step is to write the overall HSI system design specifications for each of the design topics based on the platform or equipment specifications. It is important to document how these specifications meet the detailed HSI requirements. HFE experts need to be consulted at this stage as their specific points of view on many design topics (described in Sections 5.4.3 and 5.4.4) are essential to ensure that the HSI will not impede human performance.

The following subsections provide typical design topics or subjects that are considered for HSI conceptual designs. This publication intends to provide several typical design topics or items, but these should not be considered exhaustive of possible topics.

5.4.3. Design topics driven from the HSI overall specification

The I&C attributes listed here each have an HSI design implication:

— Response time;
— Physical accessibility;
— Usability;
— Dependability of the HSI;
— Maintainability;
— Through-life management/obsolescence.

They are regarded as ‘non-functional’ requirements, but they are key technical topics to be considered for HSI basic design as they have important effects on plant personnel. For example, the response time can greatly impact the utility and the usability of the HSI. A digital system that becomes overloaded in the face of multiple simultaneous events is not a useful tool for operators. When the system is needed most, it becomes less reliable. HFE experts can help to elaborate more precisely on each of these topics to find appropriate solutions.

5.4.3.1. System response time

System response time refers to the time between the submission of an input to an HSI and the return of results. System response time in the HSI has to be defined by considering a reasonably acceptable level of human interaction needs and cognitive response.

In general, as an example, I&C systems applied to the MCR work as integrations of several layers of subsystems and the data connections between them. In such multilayered systems, response time from sensors to indications in the MCR or controls from the MCR to actuation components require time durations for sending signals back and forth.

An HFE task analysis defines task requirements, which could include response times and the need for automation. General requirements not to exceed response times may be set based on reviewing task analysis results or empirical practices on particular tasks (such as flipping display screens, screen touch responses, etc.). For I&C development input, the maximum delay time (or the acceptable range of response time), minimum and maximum frequencies of data indication, and manual control input periods are necessary, as they allow operators to perform tasks without compromising human performance effectiveness.

It may be noted that in the absence of country specific requirements, an I&C engineer may use NUREG-0700 (Rev. 2) [8] for the design requirements of system response time.

5.4.3.2. Accessibility

When considering accessibility for the operation, maintenance and testing of I&C equipment, the HSI design team needs to consider the following questions:

— Who interacts with the equipment?
— How does the user interact with the equipment?
— When is the equipment used (e.g. maintenance outages, emergency operation)?
— What tools or personal protective equipment are used to interact with the equipment?
— What is the task sequence?

A task analysis can be used to facilitate the assessment of the equipment design for accessibility, particularly to minimize the number or type of equipment pieces or components that need to be removed in order to access the desired equipment for maintenance or testing. An example of this is placing test points in safe locations on the equipment, such as power supply testing on the front of the component to prevent having to access component internals that could pose a hazard during access (i.e. voltage).

HFE anthropometric design guidance also has to be applied to ensure accessibility (i.e. considering the full range of the target audience’s body shapes and sizes that will be operating or maintaining the equipment). Typically, there are four main physical attributes to consider when evaluating a design’s accessibility:

(1) *Clearance:* How much space is available to undertake a task (e.g. for the removal of rack mounted equipment from a cabinet)? Designers need to factor in clearance for the body part, personnel protective equipment (where applicable) and the tools needed.

(2) *Reach:* How far can an end user reach to access equipment parts (e.g. heights of reach to access parts of the equipment)?
(3) *Posture:* What postures will the end user have to adopt to interact with the equipment (e.g. when accessing junction boxes, control actuators, field instrumentation for servicing)?
(4) *Strength:* What force is required to interact with the equipment (e.g. to turn a valve handle)?

Ideally, the area in which the equipment is operated also has to be accessible, meaning the location has to be free from potential hazards to personnel and the pathway has to be clear. This is particularly significant in the case of important human actions, as defined by safety analysis.

There are numerous methods and techniques that can be used to assess the anthropometric suitability of a design and it is the responsibility of the I&C team to determine which is the most appropriate for use. Anthropometric evaluation can, at its simplest, involve a paper based review of the design against the key anthropometric criteria using diagrams and information generated during the task analysis. Computer aided design tools can be very useful to assess the anthropometric suitability of a design and some computer software can enable full mock-ups of both the system and the end user. These tools can aid visualization of an assessment and provide more detailed information about the three dimensional aspects of a task.

5.4.3.3. Usability

Usability is defined as the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (see ISO 9241-210 [14]) or "[f]or a given human interface, the quality that acceptable human performance on necessary tasks can be readily achieved and sustained" (see IEEE 1023-2004 [15]). Usability encompasses the experience of the users interacting with the HSI to perform tasks. Most definitions of usability are derived from consumer products and do not emphasize the safety aspects of use. In the nuclear industry, the foremost goals of usability are safety and reliability:

— Does the HSI enable the user to complete tasks and not reduce plant safety?
— Does the HSI enable the user to complete tasks reliably (i.e. each time as desired)?

Additional goals are effectiveness, efficiency and satisfaction:

— Does the HSI enable the user to complete tasks effectively (i.e. as desired)?
— Does the HSI enable the user to complete tasks efficiently (i.e. within acceptable time windows for plant safety)?
— Are the users satisfied with the HSI (i.e. do they like the HSI)?

Usability is a reflection of the extent to which the design meets the users' needs to accomplish tasks. It includes considerations of how information is delivered to the users and how users provide their outputs as inputs to the system. The information presented to the user has to be:

— Understandable, whereby the presentation follows HSI design conventions and good practices for legibility, clarity or audibility (e.g. text needs to be sufficiently large to be legible when viewed from a determined distance);
— Salient, whereby important information is clearly distinguishable from other information (e.g. alarms have brightness and colour contrasts to stand out from non-alarmed elements in the HSI);
— Relevant, whereby the information needed is available to the user (e.g. the HSI may display key parameters constantly to have them always available to the user at a glance);
— Timely, whereby information is available when needed (e.g. the HSI does not have needless delays in presenting important information);

— Reachable, whereby the information can be quickly accessed when needed (e.g. the HSI does not feature nested windows that must be navigated to find relevant information screens);
— Accurate, whereby the information quality is assured (e.g. the user trusts that the values presented are qualified and up to date);
— Consistent, whereby the HSI style matches other HSIs (e.g. to minimize the potential for user confusion when interfacing with multiple HSIs, the HSI would not adopt its own colour scheme).

The user outputs to the HSI mirror the aspects above. For example, if the user is required to toggle a switch:

— The method of toggling has to be intuitive and understandable.
— The switch has to be salient from other switches or indicators.
— Activating the switch has to be relevant to the task at hand.
— There needs to be a sufficiently large window of time to allow the user to toggle the switch.
— The switch has to be reachable and accessible to the user.
— The switch has to function accurately as expected.
— The physical mechanism of the switch needs to be consistent with other switches.

Following these usability criteria can help ensure safety, reliability, effectiveness, efficiency and user satisfaction with the HSI. Additional usability aspects may be considered such as those found in international guidance (e.g. Refs [8], [14]) or specific guidance in the HSI style guide. The HSI style guide typically offers specific recommendations on topics such as colour schemes, minimum font size for legibility, required response times and navigation conventions.

There are degrees of usability. No design may ever forgo safety, reliability, effectiveness, efficiency and satisfaction, at a minimum. However, some HSI designs may achieve greater overall usability. Designing to achieve usability benefits from HSI V&V is described in Section 7. In particular, multistage V&V, where evaluation is performed early, can provide useful feedback to refine the design of the HSI to achieve greater usability.

5.4.3.4. Dependability of the human–system interaction

Dependability refers to the overall trustworthiness of a system (i.e. the extent to which reliance can justifiably be placed on this system). The focus here is on the dependability of the human–system interaction. Reliability, availability and safety are attributes of dependability (see the IAEA Safety Glossary [16]). The assessment of the dependability of software in nuclear power plant safety systems is outlined in Ref. [17].

The role of HFE in dependability is to minimize the potential for human errors. This subsection describes HSI design principles for preventing human errors under the different conditions of I&C system usage. Reducing the risk of human errors associated with the operation, maintenance testing and inspection of I&C systems typically involves the following:

— The broad application of HF principles and guidance to the design and modification of HSI/I&C systems (e.g. through the use of HSI style guidance — see the Appendix).
— Targeted HF assessments of risk-significant human tasks and the associated HSIs. Risk-significant human actions are those important to nuclear safety, radiation protection or radioactive waste management. They are associated with the achievement of a safety function, for example, ensuring feed to the steam generators in certain accident conditions.

The HFE assessment of risk-significant human tasks forms part of a risk proportionate approach to HFE integration, which is often adopted for large projects. This approach ensures that effort is directed towards aspects of design and operation that are most important to plant safety goals.

Risk-significant human tasks can be identified from a combination of outputs from the probabilistic and deterministic safety analyses, which underpin the safety case (i.e. the HRA and transient analyses). In particular, the qualitative element of the HRA provides important insights into the characteristics of the HSI that are required to support reliable task performance. These include the cues and indications needed by the operator to initiate actions and to confirm their success.

The types of HF assessments of risk-significant human tasks that are to be carried out are dependent on factors such as the level of maturity of the design, the complexity of the task and timescales for action. Methods include task analysis, review of three dimensional models to assess accessibility of locally operated controls and simulator (including full scope simulator) studies to assess complex actions (e.g. handling of plant transients or transfer from primary to backup HSIs and their subsequent operation). Principles for human error prevention and the error types that these principles eliminate are described in the Appendix.

5.4.3.5. Maintainability

SSG 39 [1] notes that maintainability must be considered for I&C, including location accessibility and human capabilities. It also considers interlocks, test configurations and redundancy on I&C systems during maintenance activities. In order to achieve these considerations when designing I&C systems for maintenance, the I&C team needs to address the practical HFE aspects of how maintenance has to be performed on the system.

Accessibility for maintenance and testing of I&C equipment is addressed in Section 5.4.3.2. Consistent with guidance in that section, the I&C engineer needs to consider how the maintenance personnel will interact with the components that will need to be maintained periodically, troubleshot and replaced when required. The following constraints and implications both in the MCR and especially for I&C equipment located in the field need to be considered:

- *Standardization of maintenance hardware interfaces:* Standardizing cabling, fasteners and connection points of the console port helps optimize maintenance; however, I&C engineers can design for a reduction in error by making critical connection points unique to prevent misconnections.
- *Standardization of soft control interfaces:* In a hybrid (i.e. analogue and digital) plant undergoing I&C upgrades, maintenance interfaces and controls may be displayed, function and behave differently between the individual systems. An end point vision of standardization of maintenance interfaces is desirable in regard to common interface functions with the goal of reducing human maintenance error in not using multiple different interfaces in which the control locations and behaviours are different.
- *Consideration of component positioning on equipment racking:* This is achieved by placing the components requiring frequent access for maintenance or calibration in optimal access locations. This access can then be further optimized through methods such as rail mounting of components instead of rack mounting so that the components can slide out to the maintenance staff where needed.
- *Maintenance areas to perform software maintenance and troubleshooting:* Allocating areas to perform maintenance not on the main panels and outside the MCR can be desirable to minimize disruption of operations personnel. An example of this would be a maintenance terminal for the system in an area that is separate from the primary control workstation.
- *Additional design considerations:* These include, for example, ensuring that lighting in panels and power supplies in the area for maintenance are sufficient for performing tasks.

Implications of computer security need to be considered. An example of this would be the issue of connecting laptops into plant systems or access for diagnostics and troubleshooting.

I&C engineers need to consider the design and usability of maintenance interfaces in the I&C system. This includes access to maintenance interfaces, with considerations for interlocks, maintenance

modes and security settings. This is prevalent especially in digital HSIs, which have different modes for operation, maintenance and commissioning.

As per SSG-39 [1], the goal is not to impair an I&C function while performing these tasks.

When carrying out maintenance, inspection and testing, particularly if these have to be done on-line (i.e. while the system is running), engineered barriers have to be designed to support the maintenance activity without disrupting the safe operation of the system (see Ref. [1]). In addition, administrative barriers, such as worker protection procedures, also have to be in place. Once the maintenance and testing are complete, there have to be measures in place to facilitate safe return to normal configuration. Any departure from the normal configuration has to be made apparent to the user.

5.4.4. Design topics driven from HSI functional requirements

The following design topics (or inputs) are commonly found in the HSI conceptual design:

— Information display;
— Alarms;
— Soft controls and conventional controls;
— Manual/automatic control/combination of manual and automation;
— CBPs, systems/paper based procedures;
— Computerized operation support systems (communication, operation management, etc.);
— Work environment;
— Automation level;
— Backup strategy of degraded HSI conditions.

These topics will have to make use of the HFE outputs from Section 4, especially from the function allocation and requirements. Based on these methods, HFE experts need to help the I&C team to make sense and elaborate on each of these topics. Experience shows that outputs from HFE methods described in Section 4 cannot always be directly used by I&C teams. A translation is needed. In other words, integration of HFE results in HSI design works better when HFE experts are directly involved in the I&C team.

Design concepts related to the information display, for example, have to be grouped under the ‘information display’ item. The design concepts have to elaborate how information should be displayed and may include aspects such as colour, font, size and location. The functional grouping allows all aspects of the HSI that require an information display to make use of the elements from this topic. These elements form the basis of the specification for information displays.

5.4.4.1. Information display

A nuclear power plant is a complex system consisting of thousands of items of process equipment interacting with and influencing each other in a complicated manner. An operator is a human who interacts with the process system remotely via the HSI. Operation of the nuclear power plant will typically involve multiple operators working in concert to monitor and control the plant through the HSI. Consequently, it is important that the HSI support situational awareness of all significant events occurring in the plant.

During education, training and operations at nuclear power plants, each operator forms their own mental model of the plant, which reflects a nuclear power plant’s behaviour patterns, technological and functional relationships between equipment, possible situations and appropriate methods to manage these situations. It is very important that the HSI and the operator’s mental model are consistent with one another.

The operator’s work consists in cyclic repetition of the following sequence of actions:

— Acquisition of information on the status of process equipment and process parameters.

— Analysis of actual conditions and recognition of recent situations by comparing the acquired information against mental images of the preliminary defined situations.
— Making decisions on control actions. (The operator uses operational procedures when making decisions in well known situations. However, procedures do not cover all possible operational situations. In unknown, unrecognized or untypical situations, the operator uses mental models of the nuclear power plant's behaviour to predict how these actions will affect the process.)
— Implementation of control actions and monitoring the plant's reaction.

Conventional HSIs, particularly in analogue control panels, are based on the principle of one to one correspondence:

— One item of information (e.g. process parameter value, valve position or pump state) is mapped to one HSI item (e.g. a gauge or recorder lamp on conventional panels or a mimic symbol on a display);
— One equipment component (e.g. a valve or pump) is mapped to one control (e.g. a dedicated switch or button on a conventional desk or a special window in a digital display).

Such an approach results in very extensive HSIs, consisting of thousands of components. The operator has to attend various panels (especially considering analogue technology), displays (especially considering digital technology) and other sources of information to keep situational awareness or to recognize current conditions.

There are several HSI arrangement approaches that facilitate the access, the gathering and the analysis of information with the goal of reducing the number of navigation actions and supporting decision making:

— Navigation framework facilitating display selection on displays (digital);
— Categorization and grouping of HSI components on control panels (analogue) or in task based displays (digital);
— The use of mimic diagrams on control panels (analogue) or in process flow chart displays (digital);
— Formation and representation of information (functional oriented displays);
— Representation of overview information (overview displays);
— Ecological approach to visualization of information (ecological displays displaying energy and mass balances);
— Multilayered representation of information (adaptive displays);
— Grouping of parameters (list displays);
— Representation of physical buildings or systems (floor map and mimic displays);
— Representations of the I&C logic and sensor outputs (I&C displays);
— Alert representation using alarm tiles on control panels (analogue) or alarm displays (digital);
— Instruction representations (procedure displays);
— Evolution of parameters (graph and trend displays).

Annex II provides greater detail on these approaches for VDUs capable of displaying graphics, text and other information flexibly.

5.4.4.2. Alarms

The HSI design process needs to identify the system and functional requirements of alarm displays. These activities need to be supplemented by the alarm management system design and guidance that can be found, for example, in NUREG-0700 (Rev. 2) [8], ISA 18.2 [18] and IEC 62682 [19]. Where standards do not dictate certain alarm features, HFE can provide guidance through the HSI style guide (see the Appendix). For conventional control panels such as annunciators (i.e. window tiles), HFE can provide

guidance on alarm brightness and visibility, alarm tones and differentiation, alarm tile colour coordination based on alarm importance and alarm grouping.

As I&C systems migrate to digital displays, typically HFE can provide guidance on the design of the following HSI features:

— Alarm prioritization and colour coding;
— Alarm processing (i.e. filtering and sorting);
— Alarm message content and display (e.g. active, acknowledged and cleared).

There are trade-offs between conventional window tiles and digital alarm displays. An important advantage of window tiles over digital alarm displays is that they are spatially dedicated to be continuously visible, which makes it easy for operators to detect alarm conditions. Many digital alarm systems feature alarm lists and forgo spatially dedicated continuously visible design. This may not always be desirable because the latter design may afford operators better 'at a glance' situation awareness. HFE and I&C need to work together, using a systematic approach guided by HFE analyses, to identify what variables and/or alarm conditions a spatially dedicated continuously visible layout has to provide and how that may be achieved (for example, either by conventional means or digital displays, or both).

5.4.4.3. Hard and soft controls

A control is any tool that provides the user with the ability to actuate equipment or to execute a task such as continuous adjustment or selection. Push-buttons, rotary switches, toggle switches and sliders are typical examples of conventional ('hard') controls. These require the user to perform some form of tactile physical action to change the state of the control. There are many recommendations and design principles on how to arrange conventional controls at a desk or panel. Guidance includes how to use colour, size, shape, tactile and location coding in addition to population and professional stereotype considerations, and how to prevent human errors when manipulating conventional controls. These principles can be found in NUREG-0700 (Rev. 2) [8] and IEC 60447 [20]. However, the use of conventional controls due to technological advances is gradually migrating towards the use of soft controls. A soft control is an image displayed typically on a computer screen and is activated using some form of input device, such as a mouse, joystick, trackball or touch screen. Virtual buttons, checkboxes, radio buttons and virtual sliders are examples of types of soft controls used in human–computer interaction. The following are typical actions that can be implemented using soft controls:

— Selection of objects (e.g. selection of equipment on a mimic diagram);
— Selection of options or commands (e.g. selection of a command from a menu);
— Selection of target states for equipment (e.g. selection of a radio button to specify a desired state (open/close, stop/standby/work) of equipment);
— Confirmation of intention or action;
— Smooth (using a soft slider) or discrete (using a pair of arrows or double arrow buttons) change of an analogue parameter;
— Setting the value of a parameter using soft numerical buttons.

Soft controls make an interface very flexible and compact; however, they can increase the risk of human errors. When manipulating soft controls, the user does not have the ability to obtain tactile cues or feedback. An example of this could be the control activation of a main circulation pump versus the activation of a secondary pump for domestic water supply on a soft control instead of on conventional controls. The conventional control intended for the action can have a bigger size and/or an easily recognizable shape that prevents confusion between the two pumps, whereas in a soft control interface the user clicks the same mouse or trackball button, which is not distinguishably different in the tactile characteristics of the control.

To prevent human errors when manipulating soft controls, any control operation usually requires a double action to be completed. The first action is the selection or setting of a target state or desired option, while the second action consists of the confirmation of intention expressed by the first action. Important tasks can be executed in accordance with special procedures, which assume that the confirmation task is completed by a second operator.

With the advancement of emerging technologies, there is a growing tendency among designers to apply touch screens for manipulating soft controls. Examples of these include touch screens for mobile devices, touch screens in panels in the field or large touch screens located at control desks and panels that contain all the necessary, frequently used soft controls, significantly reducing secondary activities. However, when using touch screens, the following issues need to be carefully considered in order to prevent human errors:

— The touch sensitive areas (size of button or slider) have to be of a sufficient size (usually 20 mm or more).
— Parallax error can occur due to a thick screen glass (a correction for viewing angle needs to be implemented).
— There is the risk of glare, especially when the touch screen is positioned horizontally.
— Contrast can significantly fall when the user takes a side view of the touch screen.
— Touch screens do not provide any tactile feedback, which makes it difficult to ensure that the action has been executed correctly.

Overall, I&C teams need to provide some indication when there are multiple controls. The detailed design needs to identify what the best practice is, how this may work and whether the I&C product selected can achieve the desired HSI. It also needs to consider how this might work when both soft controls and hard controls exist on a user interface. The key principle is to focus on providing the operator with the equivalent intent of certain behaviours that were useful or necessary when they used conventional controls when migrating towards soft controls for the system.

5.4.4.4. Computer based procedures

CBPs are regarded here as one type of operator support system. Operating procedures are necessary for plant operation. However, once operating procedures are applied with computer based technologies, computer aided operation supporting technologies need to be realized as an integral part of HSI systems. As discussed in IEC 62646 [21] and IEEE 1786-2011 [22], CBP functions are provided based on functional generations and/or system integrities. Industries typically recognize the following major categories and/or generations:

— *Type 1:* CBPs that are essentially stand-alone replacements for paper based procedures, presenting linked pages of static information and operating steps.
— *Type 2:* CBPs providing guidance to the operator based on information acquired by the CBP system. Every item of information may be integrated into the display formats presented.
— *Type 3:* CBPs presenting information and operating steps with full integration of on-line plant information, states and values, so that actuators can be operated from the display, automatic control functions can be accessed, and automatic execution of sequences can be initiated by the operator from the CBP display formats.

Although technologies are now able to realize the functions of Type 3, there are still limited Type 3 applications due to regulatory concerns and reliability/dependability concerns.

Procedure development guidance, which requires an operating procedure writer's guide development and procedure generation package, is generally applied not only to CBP content development, but also

paper based procedure development. HSI design guidance to specify HSI characteristics (which are discussed in this publication) is also generally applied for CBP HSI development.

The advantage of CBP applications is not only operators' support functions under the integration of a digitalized HSI system, such as a navigation hyperlink from the CBPs to a plant parameter presentation, they also bring in data storage/recording/archiving strength, which can track in-progress operation steps in multiple procedure executions and take operations logs, such as an operator's name and execution times (which will be helpful for operation administrative and safety analysis aspects).

Backup procedures, such as paper based procedures, also have to be developed to cope with abnormal situations (e.g. with CBP failures). Bearing in mind the loss of CBPs due to system failure or loss of VDUs, space has to be allocated in the control rooms for using paper based procedures.

5.4.4.5. Work environment considerations

Working environment parameters (e.g. lighting, vibration, noise, temperature conditions) affect human performance of the plant staff as well as the life of plant equipment, especially the I&C systems.

If the working environment is not matched to human needs, it can cause stress and consequently create fatigue in plant staff, which may result in human error. Historically, the feedback taken from the operating conditions of nuclear, conventional and aviation industries has concluded that the root cause of numerous incidents/accidents is predominantly due to human errors resulting from the work environment. It is, therefore, relevant to pay special attention to the working environment of the plant personnel as well as the I&C equipment during the design process.

The primary HFE goal is to provide a conducive environment for the operators in control rooms to run the plant safely through designated HSIs or I&C equipment. Any abnormal working condition can reduce the operator's cognitive and physical performance, which may lead to an undesirable situation during plant operation. Work environment considerations for I&C equipment are described in further detail in the Appendix.

5.4.4.6. Automation

The allocation of control functions between human and automation is one of the most complicated design tasks. This allocation results in the specification of the level of automation, HSI and list of control actions that need to be performed automatically. The following automatic actions are typical for nuclear power plant process monitoring and control:

— Automatic regulatory control of process parameters (e.g. automatic control of the water level in a steam generator);
— Automatic execution of step by step programmes implementing an operational procedure (e.g. turbine startup);
— Automatic activation of standby equipment (e.g. activation of a standby feedwater pump in the case of an unanticipated stop or failure of one of the working pumps);
— Automatic activation of emergency protection (e.g. turbine or reactor trip).

The selection of the most appropriate kind of automation depends on the specificity of the particular control task. The traditional point of view is that simple, well formalized routine control tasks, in which crisp logic and arithmetical calculations predominate, need to be assigned to automation, while poorly formalized, complicated tasks, which are usually performed in conditions of unclear criteria and lack of information, can be performed only by humans. Computers (or some other automatic facilities) never get tired, they work quickly and are not subject to emotions. Therefore, computers have to execute tasks that require permanent control as well as high rates and reliability of performance. Humans are able to think in a systematic manner, can easily operate with images and quickly obtain a holistic picture of situations. Therefore, humans have to perform the tasks associated with the overall assessment of situations and

conditions as well as to make complicated decisions in complex situations. They also have to perform tasks that allow them to better understand the system or to maintain skills and competencies that are crucial in exceptional situations. The Appendix provides further guidance on the allocation of functions.

5.4.4.7. I&C and HSI failure identification and mitigation

Consideration and identification of how I&C or HSI fails, how this affects system performance and how these can be mitigated by design is important. A failure modes and effects analysis is a process used by I&C engineers to identify how an I&C system fails and how this affects HSIs and system performance. The outputs of this analysis can be reviewed from an HFE perspective to determine whether HSI faults have been represented and provide recommendations for recovery from such faults.

Fundamentally, the I&C solution needs to be tolerant of human error and needs to fail gracefully (i.e. not suddenly, without warning, without a route to recovery and without severe consequences). The following are some examples of HSI faults to consider:

(a) Failure of automation
    (i) Failure part way through an automatic sequence;
    (ii) Automation misses a step;
    (iii) Automation completes a step when not all parameters are met;
    (iv) Failure to conspicuously display when a failure in automation has occurred.
(b) Failures of data display
    (i) Individual data point freeze;
    (ii) Display freeze;
    (iii) Conflicting sensor display;
    (iv) Failure to access information (i.e. poor navigation) in a timely manner;
    (v) Credible but bad data leading to possible misdiagnosis.

Additionally, the potential for I&C and HSI faults can be investigated using the following verification principles:

— Testing errors by operators to check the adequacy of the I&C system to prevent and detect errors;
— Testing recovery from faults and possible misdiagnosis of faults;
— Testing the edges of automation response capability (i.e. do the operators know where the automation limits are?);
— Testing transitions from one HSI to another (this is particularly important in considering transition to and from soft, digital HSIs and conventional HSIs);
— Testing the effectiveness of the interface to support both tactical and strategic decision making;
— Testing the impact of user configurable displays (operators are not interface designers and have a tendency to pack screens full of information);
— Zero fault testing scenarios to understand whether operator stimulation is optimized, or whether the design will lead to boredom and low vigilance.

It is not possible to design a system that never fails or prevents human error. Good HSI design can mitigate this to some extent, but it is also good practice to have a backup strategy for when things go wrong. This is discussed in Section 5.4.4.8.

5.4.4.8. Backup strategy

As required by SSR 2/1 (Rev. 1) [3], all items that are related to safety systems, safety related systems and systems important to safety should be identified and classified based on their function and their safety significance. This requirement extends to I&C systems and the HSI that the I&C system supports

(see SSG-39 [1]). However, from an operational viewpoint, plant diagnosis, action planning and controls are implemented based on integrated plant status information containing both safety and non-safety plant information. This can present some design challenges.

In conventional HSI panels, safety and non-safety HSI components (i.e. indicators, switches, controllers) are arranged in an integrated manner (i.e. arranged in mimic lines) on a safety grade panel (when safety HSI components are located on that panel) or a non-safety grade panel with safety classified HSI components distinguished (e.g. demarcated with colour codes). Therefore, operators can easily identify safety classified HSI components and continue to operate using the same control panel even when non-safety classified HSI components fail.

In a digital HSI system, non-safety classified VDUs are typically used for all non-safety class HSI components. Safety systems are maintained as separate systems and, in some cases, safety class systems may not be implemented digitally for greater security and reliability. Defence in depth needs to be carefully considered and implemented in I&C to ensure that non-safety classified systems do not impact on safety classified systems.

In the case of non-safety classified HSI failures, a backup strategy needs to be established. Non-safety HSIs benefit from redundant VDUs, such that information and controls may be brought up at various places in the control room or in secured remote facilities. The backup strategy also includes how operators identify digital HSI failure conditions. Digital HSI technologies are typically equipped with self-diagnosis functions monitoring central processing unit/memory health conditions and informing abnormal conditions as alarms. Also, periodic tests checking HSI health conditions allow operators/plant personnel to recognize digital HSI conditions during plant operations. Safety HSIs will typically feature redundant indicators and controls, but these may not necessarily be digital.

Backup HSIs need to be incorporated into normal operational use where reasonably practical to do so. This is to minimize the ‘familiarity gap’ when migrating control from the primary HSI to the backup, which can be detrimental to human performance.

Backup strategy also includes training enhancement with HSI changes (i.e. transition from normal HSI to a backup panel), automation level changes (i.e. backup manual operations in case of automation failure) and operating procedure changes (i.e. transitions from CBPs to paper based procedures or use of dedicated operating procedures for backup panels).

The transition between digital and backup HSIs needs to be incorporated into integrated system validation (ISV) trials to test the interoperability of both interface types.

5.5. ALLOCATION OF FUNCTIONS TO INDIVIDUAL HSI SYSTEMS AND COMPONENTS

5.5.1. Purpose

The purpose is to determine which HSI components, such as individual VDUs and analogue indicators, will be used to implement the HSI overall specification determined at the previous step. Some high level functions may need to be decomposed into subfunctions before the allocation can be performed.

The main objectives are the following:

— To provide human users with all the information necessary for performing their tasks while minimizing workload and enhancing situation awareness;
— To enhance the ability to detect or mitigate inadequate human actions by the HSI or by the other human operators;
— To ensure consistency of the apportionment across the HSI functions;
— To comply with the functional role allocated to each level of defence in depth specified by the I&C architecture;

— To take account of the capabilities and limitations of the technologies retained by the I&C architecture for each of the HSI systems;
— To determine the number of HSI components that are necessary.

5.5.2. Methodology

There are three types of allocation of functions to individual HSI types:

(1) The same HSI function could be associated with multiple components, which are all necessary to its implementation (e.g. a monitoring and control function could require multiple VDUs to provide the human user with all the necessary information).
(2) The same HSI function could be associated with multiple components in order to provide some level of duplication that would enhance information sharing or fault tolerance. For example, alarm presentation functions may be realized not only on individual VDUs, but also on large display panels and/or conventional alarm tiles.
(3) Multiple HSI functions could be associated with the same component (e.g. display navigation functions could be allocated to the same VDUs as monitoring and control functions).

When assigning HSI components to an HSI function, the number, performance and capabilities of individual HSI components need to be such that together they meet the requirements of the function.

Digital I&C systems are usually not developed from scratch but are based on multipurpose I&C platforms. The HSI of such platforms is designed to support a wide range of HSI functions such as information display on multiple VDUs, interaction with human users using multiple and varied input devices, display navigation, alarm signalling and management and, in some cases, computer based generic procedures.

5.6. HSI DETAILED SPECIFICATION

5.6.1. Purpose

The purpose of this step is to develop a detailed HSI specification based on the results of the two previous steps.

For digital HSIs, this would, for example, address the following:

— The display indicators and controls for each HSI function;
— The list of alarms and their displays;
— The list of procedures and their contents.

For analogue HSIs, this would, for example, address the following:

— The list of panels;
— The mimics, indicators and controllers for each panel;
— The list of alarm tiles and their locations.

5.6.2. Methodology

The methodology for this step is based on the following assumptions:

— The application of an HSI style guide (see the Appendix);
— Consistency with the I&C and plant design.

This individual specification typically contains the following:

— Function specifications (i.e. how the system behaves and how it presents information and graphic display specifications, including graphic displays, signal assignment);
— System specifications (e.g. response time, update frequency, reliability);
— Interface specifications (e.g. input/output list, signal route).

Interface specifications are developed in this phase. In a digital I&C platform, interface communication between individual systems (including subsystems) and components can be established via data networks.

Cooperation between HFE and I&C experts is very important when defining the specifications. Indeed, experience shows that the HFE contribution to system requirements is often not adequately considered. Many details are not discussed at the requirement level and will be detailed during the specification development. As a minimum, the specifications have to be reviewed by HFE experts.

5.7. DOCUMENTATION OF HSI REQUIREMENT SPECIFICATIONS

All requirements and HSI conceptual/basic design, individual and integrated system/function design specifications have to be documented and recorded to meet various needs, including configuration control (i.e. tractability, interface, revision control), design reviews and design information sharing among various stakeholders in the design process. This documentation has to be used as input to the V&V.

In the detailed design phase, all design requirements have to be met. The process of detailed design and V&V, which is described in Section 7, can be iterative to meet requirements, including the HFE analysis results, and has to be in accordance with the level of maturity of the software and hardware being considered and the extent of customization.

5.8. PROCEDURE AND TRAINING DEVELOPMENT

While not conventionally considered part of an HSI design (unless the procedure is computer based) in the context of the I&C system, misalignment of procedures and training with the HSI design can be a significant source of human error. Yet, in some design projects, the development of procedures and training is relegated to the very end of the project and is not an integrated design activity. The following subsections provide some guidance on procedure and training development as it pertains to the I&C system. The intent is to recognize the role that procedures and training play in supporting the use of the I&C system, particularly the final designed HSI. An operator has to use procedures to guide his or her interface with the HSI. Likewise, performance is shaped by training.

5.8.1. Procedure development

Once the HSI is designed, operating and maintenance procedures need to be developed to use the plant HSI during normal, abnormal and emergency conditions. This needs to include considerations for when plant systems and equipment are undergoing maintenance, testing and inspection.

Procedure development is not an exclusive HFE activity; it also engages and interacts with other parts of organizations outside the project team. An example of this is involvement with the conduct of operations in safety analysis reports. Procedure development needs to consider procedure types, structures, implementation programmes, writer’s guides, validation programmes and maintenance programmes. Procedures need to be developed ensuring that they are technically accurate, comprehensive, explicit in the actions to be followed and easy to use.

With consideration of HFE programme activities, procedure development utilizes, among others, the following main inputs:

— Task analysis;
— Important human actions;
— The already developed HSI.

Due to the fact that all power plants face design modifications continuously, a procedure maintenance programme is required that addresses procedure updates in regard to changes to I&C and the reference (configuration) of the existing I&C systems and components in the plant.

5.8.1.1. HFE inputs for procedure development

The main output of the task analysis is the description of those tasks necessary for I&C system operation, including subtasks or activities, as well as the I&C required for operation. From this perspective, task analysis is the precursor of procedure steps as it looks at the I&C required for the execution of tasks (considering HSI controls, indications and alarms as well as field components) and provides a link between the I&C and execution. In essence, task analysis is the first outline of procedural tasks required to operate or maintain the I&C system or component.

However, in some cases, experience has shown that task analysis is not always used for procedure development and examples exist of new plants whose procedures have been developed from preceding plant designs or design modifications utilizing previous versions of plant procedures. In these cases, special care needs to be taken to ensure the technical accuracy of the procedures, so they reflect the modified or new I&C system or component. Similar considerations may also exist in the case of important human tasks, in which the procedures need to focus on these tasks and on the required HSI and I&C associated with the tasks.

Overall, for the developed HSI (in panels or displays), the I&C components included need to be consistent with the outputs of other HFE activities to ensure procedure usability.

5.8.1.2. Other inputs for procedure development

Other inputs for procedure development typically include the following:

— Plant design basis or bases;
— System based technical requirements and specifications (coming from I&C documents);
— Initiating events to be considered in the emergency operating procedures, including those in the design basis;
— Generic technical guidelines for emergency operating procedures;
— Procedure writer’s guide and HF guidelines for writing the content of procedures (e.g. style guide for representing the content of the procedure, using key words consistently, how to write the steps or the level of details of the content).

5.8.1.3. Specific HFE focus in procedures

From the HFE perspective, the following features need to be considered:

— Technical accuracy, not only in terms of the tasks or activities to be carried out but also in the I&C to be used.
— Comprehensiveness in terms of relevant actions or plant conditions that exist in procedures with the affected I&C system or component.

— Explicitness in the actions to be followed (an approved list of action verbs is normally generated) and ease of use.
— Issues that can be addressed in a procedure writer's guide. (An example of guide content can include procedure structural requirements such as a statement of applicability, purpose, prerequisites, warnings, cautions, notes, steps (single actions versus continuous actions), checklists, appendices and reference material.)
— A style guide indicating how to represent the information provided in the procedures.

Paper based procedures need to support the execution of backup functions in the event of CBP failures. Moreover, in such situations, a measure has to be provided to enable operators to transition to paper based procedures and perform the procedures without confusion. For example, a hardcopy of the on-line version could be used in an identical format as the CBP, indicating steps in progress.

To ensure that the above mentioned features are incorporated and that procedures are structured, understandable, usable and consistent, a specific V&V process needs to be carried out. Apart from confirming the validity of procedures for plant operation, possible outcomes from the procedure V&V process can include the following:

— Identification of potential human errors in the procedure content;
— Timing during procedure execution that needs to be readjusted;
— Limitations in procedure information, such as notes or cautions;
— Enhancements to procedure steps that can affect the I&C, in terms of labelling, naming conventions (referenced in procedure steps).

5.8.2. Training programme development

Regular training is given to plant employees to ensure that their knowledge and abilities are maintained in the long term.

Once the HSI design and operating procedures are complete, inputs are available for training programme development. Guidance on the systematic approach to training can be found in IAEA Safety Standards Series No. NS-G-2.8, Recruitment, Qualification and Training of Personnel for Nuclear Power Plants [23]. However, it is important to consider the timeline to complete training programme executions and examinations in accordance with the regulatory/industry requirements of Member States. All staff need to be trained prior to commissioning. In a plant modification project, the impact of the modification to the training programme needs to be assessed during the planning stage. In the case of new training programmes, the longer time frame required necessitates early consideration in conjunction with the HFE and I&C development process. As in the case of procedure development, training programme development is not an exclusive HFE activity but also engages and interacts with the training organizations outside of the project team and, as an example, is integrated as part of the conduct of operations chapter in the safety analysis reports.

The training programme needs to be prepared for plant employees (e.g. control room, field operators, maintenance staff) or candidate employees, including subcontractors, especially for the maintenance training programme. The programme can utilize the outputs of previously described HFE activities for consideration in training:

— Task analysis, where the tasks (subdivided into subtasks or activities) have been identified with their specific purpose, features or requirements that are necessary to consider for training.
— Staffing and qualifications, where the types of plant employee for accomplishing each of the tasks as well as the necessary knowledge and abilities to complete those tasks are identified.
— Treatment of important human tasks, identifying those human tasks that are important from the safety perspective of the plant.

— HSI design, which is to be used during plant operation for accomplishing all operation and safety goals, considering:
  - The knowledge of how and where to access all the available information (navigation in software displays, geographical location in a conventional panel layout);
  - The different types of information available in the HSI;
  - The knowledge of how to operate the different types of control.
— The different types of procedure to be used for operating the HSI when facing different operating conditions.

With regard to I&C, training programmes need to consider specific characteristics of the technology behind the I&C and the different types of component to be used during plant operation. This includes considering normal, abnormal and emergency conditions, as well as those periods when plant systems and equipment are under tests, maintenance or inspection (especially during outages).

I&C engineering clarifications, additional information requests and modifications for ensuring human operation enhancement are topics for consideration for the design teams in regard to the link between training and the I&C system or component design and use.

Also, as training is often based on full scope simulators, the need to correctly and adequately represent the I&C in these simulators may place specific constraints on the I&C and its implementation that need to be included in the I&C requirements.

Due to the fact that power plants face design modifications continuously, training programmes will need to consider these changes prior to the commissioning of new I&C components and systems.

6. HFE IN THE PROCUREMENT OF EQUIPMENT

6.1. CONTEXT

The procurement of I&C systems is a common solution to achieving the end point vision of a design. This may be because the necessary systems expertise is not available in-house or because this enables timescales to be achieved more efficiently or cost effectively.

This section describes the synergies between the processes outlined here and in IAEA Nuclear Energy Series No. NR-T-3.31, Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications [24], including the following questions:

— How to integrate HFE within the commercial framework of a project;
— How to specify HFE requirements in the supply chain, applying a graded approach to the contractual framework;
— How to specify supplier responsibilities;
— How to specify designer responsibilities and equipment qualification and suitability testing;
— How to justify that the commercial off the shelf device meets the requirements to be installed in a nuclear power plant.

Reference [24] also provides specific information in relation to the following:

— Typical issues associated with commercial and industrial equipment;
— The procurement process for I&C equipment.

The processes and outputs identified in this section complement the ones defined in Ref. [24].

6.2. OVERVIEW OF HFE IN THE SUPPLY CHAIN AND IN THE PROCUREMENT OF EQUIPMENT

Commercial equipment procured from or designed by a third party or a supplier is referred to as commercial off the shelf. It is essential to ensure that the suppliers of equipment can provide solutions that comply with the project of an I&C system or subsystem. This section describes the key considerations for ensuring that HFE requirements form part of the commercial off the shelf product procurement strategy and contractual framework by describing the following:

— How the level of HFE importance of equipment may be determined to ensure a risk proportionate approach;
— How HFE can be integrated into the procurement process and contractual framework;
— How to specify supplier responsibilities to ensure that HFE design and analysis methods are integrated into their design process;
— How a designer may ensure that the supplier's design complies with the HFE requirements of the design.

6.2.1. HFE integration with the procurement process and the supply chain

The level of integration between the designer (i.e. the authority responsible for delivering the design) and the suppliers of equipment (i.e. the commercial entity responsible to the designer), can vary depending on the requirements of the project and the complexity of the system or subsystems being procured. For example, a large scale, complex project (e.g. a new build or a reactor inspection and maintenance system) procuring software and hardware systems will necessarily require a high degree of engagement with the supplier due to the complex nature of the requirements, the associated high degree of safety functionality and the potential duration of the procurement process. Replacement of I&C components in the field due to ageing and obsolescence is becoming more prevalent in existing plants. Although replacement of these components may have fewer complex requirements on a graded level in comparison with a large scale project, replacing these components can be challenging as they may be systemic and prolific across the plant. Examples could include the replacement of obsolete analogue protective relays or motor control centres in the field with digital I&C relays or motor control centres with touch screen interfaces. Conversely, a designer/maintainer of an existing plant that is procuring a replacement hoist for a relatively simple piece of equipment may require less engagement with the supplier due to the simpler requirements of the hoist attachment in comparison with the MCR software. Additionally, the level of HFE substantiation required by the supplier and consequently the level of surveillance by the designer may vary depending on the relative importance of the equipment determined by the designer.

It is important to identify and understand the reliance the engineering project has on the supply chain early in the design life cycle so that an appropriate HFE programme can be developed to ensure that HFE requirements are considered during the procurement life cycle.

6.2.2. Specifying HFE requirements in contracts

It is necessary to ensure that HFE requirements are appropriately considered in the procurement of equipment so that they are included within the commercial framework being applied. The HFE requirements that apply may differ for each system or subsystem depending on its relative importance, complexity and functionality. Sometimes, it may be necessary to apply a graded approach to integrating HFE requirements into the commercial framework. This is especially true in new build projects or projects that have a heavy reliance on the supply chain to provide design solutions.

The HFE requirements to be specified in the contractual framework can be tailored to suit the individual needs of the equipment being procured. This helps to ensure that no unnecessary work will be requested of the supplier and consequently reduces the surveillance burden of the designer.

To tailor the requirements to fit the needs of the contractual framework it is important to understand the purpose of the equipment being procured and how the end users are expected to interface with it.

A source of information for HFE requirements is the HSI style guide (described in the Appendix). It can be useful to specify this document in the contractual framework as part of the technical specifications provided to the supplier. Furthermore, outputs generated from HFE analysis methods, such as task analysis and function allocation, will provide the HSI basis on which to tailor the requirements. For example, a task analysis may identify a heavy reliance of the operator on audio and visual feedback from a display unit. In this case, it would be important to ensure that HFE requirements pertaining to visual and audio feedback are included as part of the contractual framework. HSI requirement documents such as the HSI style guide and any operating experience feedback from previous designs can be specified in the list of applicable documents for the supplier, where appropriate. HFE requirements in contracts have to be practical and measurable. Whether or not they have been achieved also needs to be demonstrated (e.g. through qualitative, written reports or through a simple yes/no tick box, depending on the type and importance of the requirement).

The mechanisms for specifying design requirements in contracts can be different across projects, companies and countries. It is therefore the responsibility of the I&C team to identify the mechanism for specifying HFE requirements in the procurement contract. In general terms, it is likely that a project will first offer an invitation to tender a contract (also known as a request for proposal) and then award a contract to a third party. At the preliminary invitation to tender stage, the third party may be invited to explain how they will achieve the objective of the contract. At this stage, multiple third party suppliers may compete for the contract; the designer requires an initial assessment phase to determine which candidate is most suitable. It is important that HFE is integrated with this process and that third party suppliers' responses to the invitation to tender are assessed against HFE requirements. The mechanisms for assessing third party suppliers' responses to tenders can vary greatly, and it is the responsibility of the I&C team to identify how HFE requirements will be assessed and how the results of this assessment will influence the decision to award the contract.

6.2.2.1. Specific considerations for harmonization of I&C systems

When considering different options for predeveloped I&C products, the design team needs to ensure that the software or hardware that is chosen takes into account harmonization between systems that have similar human interfaces. For example, are the new systems compatible with the old systems? What mechanisms can be used to ensure this? Some utilities use product catalogues, but these do not make it into HSI specifications that HFE provides. There needs to be some level of integration that takes into consideration the user implications of operating new systems with existing systems.

6.2.2.2. Specific considerations for modernization of multi-unit nuclear power plants

When considering modifications across multiple units (i.e. where equipment is duplicated) it is important to ensure that the I&C products that are selected are still available and supported for the next unit upgrade. For example, in nuclear power plants that operate multiple control rooms, a modernization programme may exist over a long period of time, and it is important to ensure that the equipment is available and supported from the supplier throughout the project's life cycle. Other considerations include the need for harmonization of the I&C across the multiple units in terms of interfaces due to product obsolescence or the availability of upgraded or new models. It is important to put in place a process that identifies any compatibility issues. This may necessitate engagement with the supplier during the invitation to tender phase and/or be specified in the contract for tender.

6.2.3. Applying a graded approach to the contractual framework

Applying a graded approach ensures that the level of HFE effort is commensurate with the risk of the engineering project activities related to procurement of equipment. More detailed information on the graded approach is provided in Section 2.3.4.3.

Applying a graded approach is particularly relevant to new build and complex projects that have a heavy reliance on the supply chain to deliver the end point vision. In these cases, it may not be practical from a cost, time and effort perspective to apply the same level of HFE effort to each contract or to apply a broad, single solution to a contractual framework.

The level of HFE effort required aims to be proportionate with the associated risk of the equipment being procured. For example, an I&C system crucial to monitoring, maintaining and recording core temperature may require a higher level of HFE effort specified in the contractual framework than, for example, a digital maintenance calibration tool for non-safety classified equipment. That is not to say, however, that non-safety related equipment is low risk from an HF perspective. The level of risk criteria has to be defined by HF experts prior to applying the approach. The purpose of applying a graded approach is to ensure that the right level of HFE effort is applied to the areas that are most important to the project's goals. Safety analyses provide a useful input to the identification of risk-significant equipment.

In grading HFE it is important to remember that safety classification is not always a good indication of safety relevance from an HF point of view. This is because during the operating years of existing nuclear power plants, the availability of digital technologies has significantly altered the way state of the art non-nuclear industrial process plants are operated. Some of these developments have also reached nuclear power plants and are manifest in different non-safety systems that are used for such activities as monitoring of the plant and its equipment, operative decision making and job design. For example, process monitoring systems are not safety significant per se if soft control is not utilized to conduct operating actions. Nevertheless, process monitoring systems are vital for the formation of situation awareness of process operators and, therefore, require significant HFE efforts. Other obvious non-safety systems requiring HFE efforts include electronic procedures and maintenance management systems. In the case of maintenance management, a human error in maintenance job design may cause a maintenance error even though the job design system as such is not safety significant. Digital systems used in nuclear power plants have, therefore, also to be analysed concerning indirect safety implications when grading the HFE programme.

6.2.4. Specifying supplier responsibilities

At the beginning of the procurement process it is important to define what the responsibilities of the supplier are in relation to HF. Generally, this involves requiring the supplier to demonstrate that HFE has been considered in the design and that their design satisfies the HFE requirements of the I&C equipment. Specifically, the supplier responsibilities need to be commensurate with the risk level of the equipment. For example, if the equipment being procured has a related human action important to safety and a high degree of human interaction, it may be necessary to request a high degree of design compliance, demonstration and substantiation by the supplier.

The exact activities required by the engineering project from the supplier are context dependent, and it is the responsibility of the I&C team to determine what level of compliance, demonstration and substantiation is required. The following are examples of supplier activities that can be requested as part of a contract to procure I&C equipment:

— *Compliance matrix:* This would demonstrate compliance/non-compliance with HFE requirements.
— *HFE plan:* This plan would detail the supplier's work programme to ensure that the HFE requirements in the contract are met. It could include timescales for implementation, details of HFE assessment and evaluation methods, define key stakeholders and their relationship with the project and detail how the HFE work programme aligns with the project's milestones and end point vision.

— *Design substantiation reports:* These reports would summarize the HFE assessments and reviews that have informed the design process and would include details of any task analysis, function allocation and design reviews.
— *HFE design reviews:* These would include supplier led HFE specific design reviews to be held both internally by the supplier and externally between the supplier and the designer.
— *HF focused tracking system:* This tracking system would be the log of all HFE specific design assumptions and issues and would provide a historical record of when these were raised and how they were addressed in the design (see Section 2.3.3.8).

It is worth noting that providing suppliers with templates or examples of expected outputs can improve the consistency and adequacy of supplier deliverables. For example, designing a compliance matrix that would be sent to suppliers would ensure consistency of the responses and ensure the right level of detail is provided.

6.2.5. Specifying designer responsibilities

The designer may specify to the supplier how they review the work undertaken by the supplier and what mechanisms will be implemented to assist the supplier to achieve the end point vision of the design within the scope of their contract. The exact activities required by the designer depend on the contract being implemented and the requirements of the project. The following activities are examples of what an I&C team may choose to implement to ensure that the supplier achieves the end point vision of the design:

— *Attendance at design reviews:* The designer may want to specify attendance at supplier design reviews. This could be for HFE specific and for general design reviews and could align with specific project milestones.
— *Review of supplier outputs:* The designer may want to identify specific supplier outputs for review. These could include design reports, the HFE plan or equivalent, HFE issues register or log and the compliance matrix.
— *Final acceptance of design:* The designer may specify, depending on the relative importance of the equipment, how design acceptance will be achieved with the supplier.

6.2.6. Equipment qualification and suitability

Requirement 30 of SSR-2/1 (Rev. 1) [3] states: **“A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.”**

The HFE aspects of equipment important to safety need therefore to form part of the equipment qualification and suitability analysis. The equipment qualification process may be defined by other project stakeholders, and it is important therefore to identify this process during the HFE planning phase and ensure that HFE activities and outputs support it.

In the procurement of equipment, it is important to specify that HFE analysis will form part of the equipment qualification and suitability analysis. This process can be phased depending on the scale and scope of the engineering project and may occur at different design maturity levels.

7. HFE VERIFICATION, VALIDATION, IMPLEMENTATION AND OPERATION

7.1. INTRODUCTION

The main objective of HFE V&V is to guarantee that the final design conforms to the accepted design principles and safety and design requirements for human operation. It ensures that the I&C components or systems, with special consideration of the HSI, are adequate in enabling plant personnel to successfully perform their tasks, assuring implementation of the design goals. This section complements SSG-39 [1] for existing I&C V&V activities.

When considering new builds, design modifications and decommissioning, all I&C (not just safety or safety related systems) requires testing, evaluation and V&V. SSG-51 [2] provides high level information on how to perform V&V. It is best used by design and independent teams throughout the design process in an iterative manner instead of just as a final design evaluation at the end of detailed design. This is different from I&C technical testing and evaluation executed during design. V&V needs to be integrated into the design process but does not replace normal quality assurance processes such as factory acceptance testing.

This process is best optimized by a graded and multistage approach to V&V from the beginning of the design to design completion. The graded approach means that not necessarily all possible evaluations are performed but rather those with the most safety relevance. This approach allows early testing findings to be addressed and incorporated into the design process to optimize it and prevent the need for reworking. The multistage approach means that evaluations are conducted across the design's life cycle, typically in an iterative manner, as the design evolves and is refined. This multistage process creates efficiencies in crediting all tests, evaluations and V&V that are performed throughout the design process. Typically, V&V culminates in a summative evaluation of operator performance or ISV using the HSI.

7.1.1. Strategic scheduling

V&V scheduling is best incorporated when it is specifically aligned with the necessary design activities within an overall engineering project, while considering time frames and interactions with other engineering teams. Planning for HFE V&V needs to be initiated as soon as possible within a project to ensure that a multistage iterative V&V approach is incorporated early in the design process. Testing and prototyping are fundamental to ensure that requirements are correct before any design is implemented.

It is important to have requirements that are validated before they are implemented, due to the fact that once implemented, any modification to the installed I&C is extremely costly. Alignment of these activities results in developing efficiencies for the cost–benefit to the I&C project. This is achieved by integrating the HFE V&V with I&C testing activities. This allows the I&C team to take advantage of and credit HFE user/usability testing instead of requiring separate isolated HFE testing, and provides early confirmation of meeting requirements.

In order to develop V&V as an iterative, multistage approach, it is good practice to follow a plan that considers the development process in terms of the following:

— Complexity of components;
— Hardware and software HSI interactions;
— HSI interactions for multiple systems;
— Plant location;
— Project schedule;
— Installation time frames.

In practice, the necessary V&V activities are planned and inserted into the schedule after the HFE design and analysis becomes available, which, along with project milestones, allow specification of start dates, duration, outputs of deliverables and schedules of revisions to be issued. Embedding time to address deficiencies and discrepancies within the project schedule's technical activities is essential due to the impact on project design implications.

The time frame for addressing HFE deficiencies or discrepancies needs to provide for the rationale of accepting or rejecting the HFE design recommendations. This scheduling buffer allows the design team time to modify the I&C components or system when a design iteration or revision is needed. Time for deficiency and discrepancy management has to be embedded within the rest of the technical V&V activities during the project planning stage in order to obtain benefit from an iterative V&V and design process and to not result in significant negative schedule and cost impacts.

V&V planning and scheduling also need to consider that not all testing activities conclude at the end of detailed design. There is the potential that some V&V activities might be unable to take place until the commissioning and installation stage. The schedule has to include provisions to complete the remainder of outstanding V&V activities that could not be evaluated until installed at the site.

7.1.2. V&V planning

In terms of project planning, HFE V&V considers the following:

— Objectives;
— Scope;
— Strategies;
— V&V activities (with their respective inputs and outputs);
— V&V team training (i.e. the V&V team has to be independent from the design developers, which means the designer of the I&C is not part of the validation evaluation team but is available to provide technical support during validation);
— Operating crew test participants and their composition (i.e. the test participants have to be independent from the subject matter experts who provided input into the design);
— Schedules;
— Project deliverables;
— Technical task execution;
— Relationship with other engineering activities, such as the I&C activities.

The main technical activities in consideration for HFE V&V include the following:

— Identification of HFE standards and guidelines during the planning stage;
— Review of design requirements, drawings and manuals during the HSI design stage or earlier stages;
— Task support verification;
— HFE design verification (i.e. HF guidelines compliance and anthropometric evaluations);
— HFE system validations (e.g. performance based evaluations with preliminary usability testing, iterative and integrated validations).

The scope of HFE V&V covers all HSIs and is not limited to safety or safety related systems. Non-safety related balance of plant HSIs (i.e. not just the MCR) are also in the scope of V&V activities.

Traditionally, V&V occurs at the end of the design process. This may seem an effective way to minimize the cost and time required for HFE evaluation. However, restricting V&V to the end has the potential for significant cost and schedule impact. If significant discrepancies, deficiencies, human errors or usability issues are identified during V&V, this may require redesign and other rework activities, which can lead to schedule delays. Therefore, to minimize the potential for such delays, it is advantageous to follow a multistage, iterative approach. This allows for a range of HFE evaluations to be credited

throughout the design process and issues to be identified while there is sufficient time to correct them. Starting with early usability testing, suitability testing and user reviews during concept testing, following an iterative design and evaluation process, then culminate in final V&V.

A practical example of this iterative, early usability testing has been used in both outage maintenance in reactor vaults and in decommissioning, in which low grade simulations (such as cardboard boxes in a mock-up and paper interface) can test accessibility and positioning of instruments and I&C system components. This helps test I&C suitability prior to installation in challenging environments and its impact on personnel safety implications. Virtual mock-ups can also be used to safely conduct early validation testing.

Evaluations early in the design stage allow for early incorporation of elements and components into the design. Such formative evaluation establishes the usability and suitability of the design and minimizes effort at the end. The end goal is to provide results as early as possible and, at the same time, allow traceability in design evolutions.

Multistage, iterative V&V may not be applicable for small modifications and may be more useful in large modernization modifications and new builds. It is best optimized for a design life cycle that allows sufficient time for evaluations and latitude to allow incorporation of design changes. When implemented, it provides V&V results earlier to the design team with the advantage of allowing design changes to be executed and implemented without schedule disruptions. It additionally avoids replicating or propagating HFE deficiencies or discrepancies in subsequent HSIs being designed throughout the system design process. Initiating alignment with the design development schedule during V&V planning necessitates continuous interaction with other design teams while facilitating a consistent application of HFE criteria throughout the design process. This allows the design team to address deficiencies in a timely manner to prioritize, document and solve or disposition them for acceptability.

7.2. HSI VERIFICATION

Verification is the comparison of a design against an external standard. The verification process is used to demonstrate that the I&C component or system has been designed as intended, consisting basically in two main activities as outlined in SSG-51 [2]:

— Task support verification;
— HSI design verification.

Other aspects of verification ideally consider a verification that provides confirmation that all design recommendations have either been implemented in the design or dispositioned as acceptable by the HFE and project team. Verification of the as-built design is discussed further in Section 7.4.1.

7.2.1. Task support verification

The main objective of task support verification is to check the I&C component and system usability for plant operation and maintenance personnel. A task support verification takes information from the function and task analyses relating to the I&C needs of the system user and compares it with what the designed system both provides (i.e. information) and offers (i.e. control).

In performing a task support verification, the function and task analyses (as discussed in Section 4) and HSI are compared for compliance, considering the HFE requirements for plant operation purposes and identifying those deficiencies or discrepancies found for subsequent analysis. Task support verification focuses on the following elements:

— New components in new systems;
— New components in existing systems;

— Interim, temporary configurations of components and systems for modifications and modernization;
— Systems resulting in the addition of new operational demands.

The task support verification results need to provide confirmation through systematic and correct HSI design for plant operation, following the task analysis and function analysis documents. Task support verification may require supplemental information not included in the task analysis reports, such as piping and instrumentation diagrams, logic diagrams and system engineering specifications from I&C and process engineers.

Typical task support verification discrepancies and deficiencies found in utilities include the following:

— *HSI inventory inconsistencies:* The inventory of alarms, indications and controls may not be consistent between the task analysis reports, function analysis reports and HSI reports.
— *Incomplete task analysis and/or function analysis inventory:* The analysis, with the inventory of components, may not have defined the minimum inventory considered sufficient by the V&V team for plant operation.
— *HSI component properties:* Component properties or features may not meet the requirements associated with a given task for adequate performance.
— *Components present in the HSIs, but not justified in the task or function analyses:* Sometimes this happens due to late hour requirements (such as operating experience preferences, reference plant inputs or specific procedure execution requirements).
— *No consistent results for similar issues:* This may happen due to verifier preferences.

For certain engineering projects a task analysis may not be available, but usability verification is still required. In those cases, task support verification is best carried out by comparing the new HSI with operating procedures (existing or new) or by reviewing the HSI with operation and maintenance personnel. I&C engineers need to be aware of the use of I&C inputs for carrying out this activity. The found discrepancies, as outputs of this verification, may point to I&C engineers for consideration and may require changes in the I&C and associated HSIs.

7.2.2. HSI design verification

HSI design verification is an evaluation to verify that the HSIs are designed to accommodate human capabilities and limitations because they conform to HFE guidelines (see NUREG-0711 (Rev. 3) [25]). (It needs to be noted that HSI design verification does not guarantee that an HSI is operable for the tasks to be performed, only that it complies with HFE guidelines.)

HFE compliance has to be proven in design modifications for new HSI components or new layouts within an existing design or in existing plant equipment. The features of a new component used for replacement require confirmation in order to avoid undetected new features that could potentially introduce inconsistencies or non-fulfilment of HFE guidelines.

Typical industry HFE guidelines used for design verification are included in the following references:

— NUREG-0700 (Rev. 2) [8];
— EPRI 3002004310 [9];
— ISO 9241 series [26];
— ISO 11064 series [27];
— MIL-HDBK-759C [28];
— MIL-STD-1472G [29];
— IEC 60964 [30];
— Style guides.

It needs to be noted that these HFE guidelines only address HFE aspects of design and are not guides for I&C.

The HFE guidelines to be applied for any design are country and plant dependent, with the following specificities:

— Normal practices are that HFE guidelines applied are those of the plant and country where the design has been developed, and in some cases may be endorsed by the corresponding regulatory body where the design is being implemented.
— The absence of HFE guidelines in a country does not preclude a design to be verified, and equivalent guidelines have to be defined or identified.
— For modifications to existing plants, these plants may have style guides or design guidance conventions that may be specific to their type of plant or specific utility. This can be due to existing plant conventions or design conventions present, in which the operations and maintenance users are accustomed to conventions. Changing to other standards may introduce significant human error opportunities by advocating new HSI conventions at the plant.

The availability of an existing or legacy guideline does not preclude the need to comply with updated HFE requirements. Choosing to maintain outdated HSI design conventions and HFE guidelines versus adopting current best practices needs to be carefully weighed. Small I&C updates may not warrant significant overhauls in other aspects of the HSI. Larger I&C updates will generally seek to apply current HFE guidance. Wherever possible, significant HSI changes (e.g. digitizing parts of analogue control panels) need to remain within the system being modified (e.g. a digital turbine control system would introduce a distributed control system HSI to that system only, not across all boards). Interface consistency is the overriding principle to maintain. Keeping interfaces consistent within particular systems minimizes the opportunity for operator confusion. If a new design is being recommended contrary to plant conventions, it is advisable to add this design feature to the plant HSI style guide in future designs.

Typical HSI design verification discrepancies and deficiencies include the following:

— Discrepant HSI that simply does not match the HFE guidelines;
— Discrepant HSI due to different design criteria (e.g. following the same HSI style guide but implemented differently);
— Discrepant HSI when primarily based on a design specification that has not considered HFE guidelines;
— Discrepant HSI lingering after trying to address a previous discrepancy;
— Outdated discrepancy (when a new design revision is issued, planned or unplanned);
— Discrepancies in the HSI design verification will likely require changes in the I&C and associated HSIs.

Annex III includes methodological aspects related to the execution of the HFE verification.

7.2.3. Applicability considerations related to verification

A task support verification is always applicable for new builds, but in the case of design modifications, verification may depend on their scope and complexity:

— When design modifications only involve replacing equipment with the same functionalities, the task support verification is not applicable or required.
— When operator tasks remain unchanged in a planned design modification with no new demands on the operator, the task support verification may not be applicable.

— When the modernization involves changing the HSIs from analogue to digital, the evaluation of HSI secondary activities (such as the operator physically moving to access information) may not be relevant to task support verification.

The types of guidelines to be considered are described in Annex III.

7.2.4. Graded approach considerations related to verification

Engineering project leaders may wish to consider a graded approach with regard to the scale that is practical for verification. This is because of the complexity and number of interfaces involved in an engineering project. A graded approach considers which type of evaluation fits the needs of the project at a given stage of its design. For modernization activities, it may be sufficient to conduct verification activities during early design phases followed by validation exercises at the end of the design.

New builds involve a high number of HSIs that have to be verified to increase confidence in an error free design. However, in some cases this may be impractical or difficult to achieve, so the verification effort needs to focus on selecting an HSI sample that is representative of what is being designed. The sample could focus on those HSIs that are:

— Safety related;
— More frequently used;
— Cover all the different technologies and HSI types.

7.2.5. Verification outputs to I&C

Because of a possible impact on the design and schedule, it is important to communicate any design recommendations and discrepancies discovered through verification as early as possible. As with the outputs of the HFE analyses, issues and recommendations need to be tracked, allowing for their resolution or disposition. Any discrepancies or recommendations that have not been resolved by the end of the detailed design need to be tracked by the project team before moving into the construction, commissioning and implementation stage of the project.

7.3. HSI VALIDATION

Validation is a confirmation that the design meets the performance objectives of the system and plant. Validation is carried out with performance based evaluations of the HSI design. System performance is observed, often through ‘operator in the loop’ studies. Performance is measured in terms of the plant parameters obtained and personnel tasks performed, as well as with the results of communications and coordination activities, situation awareness, workload (both cognitive and physical) and anthropometric and physiological factors. As a consequence, validation is the process that determines whether the designed HSI achieves the overall system goals. It is not only executed in the evaluations of designs for the MCR, but it is applicable to other control centres and to I&C components and systems throughout the entire plant. In essence, it confirms that the equipment meets the suitability and requirements and is usable for the end users across the plant.

HSI design teams can take advantage of the results being incorporated into I&C functional testing. This allows teams to take credit for HSI validation testing in the early stages of I&C development and prototyping, in which early usability testing can be executed. This allows the team to avoid repetition or to question issues already tested. Tests and evaluations build on each other and are not isolated from the final validation process. By taking credit for previous testing, the final validation can take advantage of the efficiency and length of the testing.

For validation, a plan or procedure is usually developed ahead of time describing the stages, methods to be followed and also acceptance criteria that may be requested by regulatory bodies or plant owners. At a minimum, an ISV has to be performed on the HSI, including an evaluation of end user interactions with the system. Additional validations earlier in the design will help shape and improve the design of the final HSI.

7.3.1. Validation preparation

Validation needs to start with an implementation plan that describes the following, as outlined in SSG-51 [2]:

— The scope of the evaluation;
— The schedule, considering the different stages (as applicable);
— The test environment (or potentially multiple environments for a multistage process);
— Personnel required, including the validation team and crew (or other participants);
— The training needs;
— Scenarios and tools;
— The necessary data collection and analysis methods (including measures of effectiveness);
— Evaluation and acceptance criteria (including requirements fulfilment).

Annex III includes methodological aspects related to the execution of the HFE validation.

7.3.2. Multistage validation

In large and complex projects, such as new builds, an HSI multistage validation process can be planned in order to start validation as the implemented HSI design becomes available. The primary advantage of this multistage approach is that it provides results early during the design phase, when changes are easy to make. During stepwise approaches to plant modernization, validation planning needs to align with the migration and implementation strategies of the I&C components in which each interim configuration needs to be validated either through subsystem validation or ISV. As a design evolves, the level of rigour of the validation exercise may increase. Early stage validation may involve mock-ups, interim validation may make use of prototypes, and late stage validation should ideally use actual systems, when available.

7.3.3. Graded validation approach for modifications

Validation is always applicable for new builds, but for design modifications applicability may depend on the following:

— Regulatory requirements;
— Type of design modification;
— Importance of systems being modified;
— The way the plant operation is modified (especially applicable if operator tasks are greatly modified, for example, in modernizations);
— Safety class of the systems involved in the design modification (e.g. non-validated modifications related to non-safety systems can change tasks, affect other HSIs, degrade operator performance).

The graded approach to validation allows for the level of validation effort or applicability to be commensurate with the complexity of change without the need to execute a significant level of HFE effort when it is not warranted. Examples of three grades of validation for modifications are described below:

— In a limited validation, participants are provided with information on the design change. The nature of the proposed change will determine the most appropriate way to present this information. The validation team describes impacts of the change on tasks that the user group would have to perform. Participants are asked to review drawings, pictures, procedures and other available static job aids and talk through the proposed design/interfaces.
— The standard validation is an additional step up in complexity from a limited validation, requiring more preparation and having more detailed pass/fail criteria. The participants are provided with information and/or training on the design change. The participants carry out a dynamic walkthrough or talk through of the proposed design to support actions required within a scenario or scenarios. This can involve a mocked-up interface or control area for which the validation or other project team members provide information about system response if a functioning simulator is not available. Typically, the participants will simulate the task by verbalizing their actions of the execution or procedures (draft or not) or expected task steps. This simulation is then evaluated by the validation team.
— Full validations often use some level of simulation or mock-up and often have objective pass criteria (e.g. time to complete a task, successful completion rate, detection of an abnormal condition) in addition to the subjective criteria used in the less involved validation levels. It is not uncommon for participants to require some training or a detailed introduction related to the validation exercise, prior to actual trial participation.

Graded approaches to validation can be used in a multistage manner with a lower graded approach or with pre-validation requirements during concept testing or early prototype design, and with a full validation at the end of the design.

7.3.4. HSI validation outputs to I&C

The consequence of these performance based evaluations is that the HSI is tested with representative users, any discrepancies are tracked, and design recommendations may be recorded to improve the design. Quantitative findings (e.g. time to complete a task or operator situation awareness) may be mixed alongside qualitative findings (e.g. operator feedback on preferences or design improvement suggestions). Example findings might include the following:

— I&C logic not working correctly;
— Display colours not readily highlighting abnormal states;
— Signals missing in the I&C logic to meet safe operational goals;
— Key information not easily found on a digital display;
— Hardwired component design not meeting user expectations or enabling operator errors.

Those validation results that are issued as discrepancies need to be addressed and dispositioned prior to finalizing the design.

7.4. IMPLEMENTATION V&V DURING INSTALLATION AND COMMISSIONING

The evaluation of I&C components and HSIs is not complete at the end of the detailed design and V&V. After the previous activities within the HFE programme are completed, there are generally procedures and processes in place to manage the construction, implementation, installation, commissioning

and declaration of ‘available for service’ activities. In a broad sense, these all can be referred to as the ‘implementation’ stage of the project. This also includes verification of interim configuration states, when the I&C components within a larger I&C modernization project are being operated prior to completion of the entire system. An example of this would be digital replacements for analogue controllers being introduced through multiple outages, in which the new I&C controllers are used after each subsequent outage until the modernization is complete.

7.4.1. As-built V&V

As part of the implementation stage, design teams need to consider the as-built V&V of the state of the equipment in the field after installation. As-built V&V is important due to the fact that there may be unanticipated discrepancies between the drawings and installed field configurations. There is a potential for changes in the equipment during the field installation that can impact HF considerations and are not in the analysed configuration. This includes examples of the following potential environmental factors and other concerns:

— Ventilation;
— Noise;
— Illumination;
— Spatial constraints;
— Limitations due to surrounding equipment;
— Accessibility if the field location is different than in the design;
— Relocation of I&C component placement or orientations;
— Configuration changes in equipment layouts;
— Use of different HSI components.

From this perspective, the HFE team needs inputs from any other engineering team, such as the I&C team, in order to identify implementation changes compared with the design. The HFE team determines whether the installed I&C system will have a significant impact on the user due to differences from the intended design.

The design team may also need to address open activities coming from the previous V&V process. It may include steps that could not be completed until implementation due to conditions at the location in the plant that could not be simulated during factory validation.

The changes identified as acceptable during the as-built evaluation have to be reflected in plant drawings and materials (such as training material, procedures, drawings, simulators, etc.) to maintain configuration control.

Any new identified HFE issues may require further V&V with a suitable plan for resolution.

7.4.2. Acceptance criteria

In principle, the as-built V&V needs to address the following intentions:

— All HFE related issues identified prior to HSI design implementation have been adequately addressed.
— Any new HFE related issues have been identified and documented.
— A suitable plan for resolution has been addressed.
— Any remaining non-conformances have been assessed and deemed to be acceptable.

HSI discrepancies or unforeseen issues identified during the as-built V&V need to be addressed prior to turning the I&C component or system over as available for service.

7.5. HUMAN PERFORMANCE MONITORING AND ITERATIVE DESIGN

The monitoring of human performance needs to start after the design commission is completed to guarantee that the implemented and commissioned HSI maintains the same conditions as when it was verified and validated.

Human performance monitoring is required as per the HFE guidelines to ensure that no significant degradation occurs because of any changes that have been made after the ISV in the plant and to confirm that the conclusions drawn from the ISV remain valid. The monitoring of human performance needs to remain an active and ongoing process to evaluate the continuing effectiveness of the design to properly support personnel in carrying out their work tasks safely and effectively. The issues identified during human performance monitoring can serve as a significant input for the improvement of the design.

8. SUMMARY

The objective of this publication is to provide design teams (including I&C and HFE disciplines) with practical strategies and methods to consider during I&C system design that will result in improved HSI design. This guidance is delivered using a structured, systematic and interdisciplinary framework, which aligns with the I&C life cycle [1] and the progression of the HFE programme [2] within an engineering project. The key elements of this framework are summarized here:

— Development of an end point vision, which places an emphasis on how the I&C system design can support plant operational, maintenance and management strategies early in the engineering design process;
— Planning of the activities associated with an engineering project, focusing on the HFE programme and on where interfaces between I&C and HFE regarding inputs and outputs need to be considered;
— Derivation of HSI design basis requirements, which has to entail a comprehensive review of relevant codes and standards, consideration of technology platforms and high level considerations coming out of preliminary HFE analyses;
— Development of HFE requirements and recommendations through analyses that form an important input into the HSI design process;
— Design of the HSI using a systematic approach that harmonizes requirements for an overall HSI design before specifying individual HSI characteristics;
— V&V of the HSI design and integration of the systems using, where possible, a graded and multistage approach before installation, commissioning and operation.

This publication recognizes that engineering processes, when executed, are not always linear and sequential but iterative and can sometimes be in parallel. It provides guidance on where and when in the design process such iterations and refinements may occur, but this may need to be adapted to meet the needs of the organization. However, the intent of the guidance is clear:

— HSI design is an integrated process that includes complementary activities between multiple disciplines at multiple stages of design. A team based approach is paramount to the success of I&C system design. This publication focuses on HFE and I&C interfaces but HSI design also involves engagement with other disciplines, as described throughout.
— Engineering projects with an I&C and consequently an HSI component vary in scope. Understanding this reality, this publication considers differences in the application of activities described for new builds and modifications, including modernization.

— With the expanded capability and flexibility of I&C technologies and the introduction of emergent smart products into a nuclear facility, the use of HSIs that come with these products has to be considered in scenarios beyond the control room.

The evolution of I&C technologies with digitalization has allowed for greater integration and interaction of functions needed for enhanced operations and maintenance. Engineering design, particularly for I&C systems, has to capitalize on this opportunity in order to produce an integrated HSI design that will support operations and maintenance, and in general, will optimize safe and productive human performance within a nuclear facility.

Appendix

SUPPLEMENTAL GUIDANCE ON SELECT HSI DESIGN TOPICS

A.1. DEVELOPMENT OF USER POPULATION DESIGN RANGES AND HSI STYLE GUIDES

A.1.1. Development of user population design ranges

I&C systems and components need to be designed so that they can be operated, maintained, inspected and tested by the intended user population under the anticipated conditions. The intended user population or end users of a system will comprise a broad range of different physical characteristics, including size, shape, reach, posture and strength. For example, arm length, and therefore functional reach, can vary greatly. The range of functional reach of the user population can help to determine how to design workstations so that equipment is accessible and displays are readable.

Equally as important as the physical characteristics are the conditions in which the equipment operates as this can determine the personal protective equipment worn by operators or maintenance personnel. Personal protective equipment can increase the end users' physical dimensions and restrict movement, reduce zones of effective reach and decrease tactile feedback.

If the physical dimensions and the conditions of operation are not considered in the design of an I&C system, the number of people who can effectively use the equipment will be reduced; in the worst case scenario the equipment could be rendered inoperable simply because the end users are physically unable to interact with it.

I&C requirements, therefore, have to consider both the physical aspects of the end user and the conditions in which the equipment will be used to ensure a usable design. HF experts can be particularly helpful by providing information on anthropometric aspects of the end users and the conditions in which they work. Additionally, HF experts have to help I&C experts evaluate and define design solutions that take these constraints into account.

Anthropometric evaluation starts and ends by answering three basic questions:

(1) Who is in the user population?
(2) What range of the population should be covered by this design?
(3) What design constraints affect the usability of the design?

The end user group of an I&C system has to be defined prior to the specification of the design. User population design ranges describe the physical and cognitive attributes of the end users specific to that system. These could include, but not be limited to, the following:

— A comprehensive range of body dimensions covering all aspects of the human body (e.g. arm length, sitting height, sitting knee height, shoulder breadth);
— A definition of how people with physical limitations will be accommodated and a definition of the appropriate anthropometric dimensions (e.g. wheelchair width);
— Inclusion of functional aspects of the human body's physical dimensions, such as reach and strength;
— Inputs from staffing analyses carried out (e.g. roles and responsibilities, training expectations; see Section 4).

The physical characteristics of end users can differ by country; some countries may have a population with a high range for standing height and some countries may have a low range for functional reach. This is especially important when considering the design of nuclear power plants for multiple

countries, which is common in today's industry. The design of a system for a specific user population may be suitable for one country but may not be as suitable for another.

It is useful to define the user population design ranges prior to the specification of the design as it will help the I&C team to understand the physical and cognitive limitations of the end users. However, it is sometimes difficult for the I&C team to make sense of this information and to translate it into design specifications. HF experts can help, as this is part of their key expertise.

Defining the user population is also crucial for the HFE requirements development process and acts as a tool to develop appropriate HFE related ISV programmes.

A.1.2. HSI style guide development

There are multiple information sources that can be used to develop an HSI style guide and it is important to define a clear scope of applicability before defining the content of the guide. The content of the guide will be defined by the requirements of the project, the design requirements of the system and the end user requirements. To help develop system understanding and user interfaces that form the basis of the HSI style guide, the following information sources (or equivalent) can be used:

— *Concept of operations:* This provides information about the purpose of the I&C system, its intended use and operational life cycle, which can help to define areas relevant to the HSI style guide.
— *Safety HSI functional requirements:* These provide information about safety critical functions undertaken by the system. They can help to identify which HSI elements of the system will have safety critical functions.
— *I&C requirements:* These provide information on requirements for the I&C system and HSIs.
— *Task analysis:* This provides information about human–system interaction, which can help to define user needs, the conditions of operation and the requirements for the HSIs.

To help develop the HFE requirements and technical detail in the HSI style guide, the following information sources can be used (among others):

— IAEA SSG-39 [1], which provides specific technical and safety related information about I&C systems.
— IAEA SSG-51 [2], which provides information about HFE engineering aspects of nuclear power plants that can help to define the relevant areas of the HSI style guide and information on how to achieve certain HFE related tasks (e.g. the task analysis).
— NUREG-0700 (Rev. 2) [8], which provides a large set of HF guidelines in many areas to be fulfilled in the nuclear field, particularly for US designs.
— International standards and guidelines that provide detailed information about specific HFE technical areas (e.g. human–computer interaction, alarms, MCR design, CBPs; see, for example, Ref. [27]).
— HFE requirements and conventions in design and operational documentation for existing plants. Plant walkdowns can also be used to collate information on the HSI design requirements and conventions.

A.1.3. Content of an HSI style guide

An HSI style guide can be tailored to the requirements of the engineering project or plant. For example, a nuclear new build project would require a comprehensive suite of HFE requirements covering all aspects of the design from the MCR to local field HSIs. It would specify the colour coding conventions to be used for alarms in the MCR through to the positioning and location of labels on conventional annunciator panels in the MCR and field locations. Conversely, if an existing plant is looking to modernize an MCR, it may be necessary to develop an HSI style guide that covers specific technical areas such as software architecture, workstation anthropometry and display devices. The scope and applicability of the guide have to be clearly defined at an early stage of development.

An HSI style guide may cover a variety of HFE technical areas that could include, but need not be limited to, the following:

— *Context of use:* A definition of the scope and applicability of the guide. This is to specify who will use the guide (e.g. in-house designers, suppliers, HFE specialists) and for what purpose. It may also include a description of how to determine the relative importance of requirements, examples of V&V activities and any limitations of use, such as the duration of applicability.
— *Human–computer interaction:* For example, software architecture, displays, software/hardware integration, hard and soft control systems.
— *Environmental considerations:* Light and glare, thermal environment, noise and vibration.
— *Anthropometric considerations:* User population body size definitions, sight lines, reach zones, maximum and minimum space considerations and working envelopes.
— *Alarms:* Rationalization and prioritization, inhibition and shelving, flooding and nuisance alarms, alarm displays, audio and visual considerations, alarm coding, alarm severity, reliability and maintenance of alarms and computerized alarm response procedures.
— *Information coding and display:* Software and hardware coding; colour, size, shape and spatial coding; alphabetic, alphanumeric and numeric coding; graphical displays; font and text; labelling; computer and paper based procedure formats.
— *Automation:* Role of operators with an automated system, system response and feedback, monitoring, fault detection, override and emergency stops.

The HSI guidelines need to be written cooperatively by HF experts and I&C experts as this document has many implications for both of them. For example, graphical animation in a digital HSI is performed by an I&C platform, so if HF experts note a requirement that some information has to blink at various frequencies, the I&C platform will have to comply with this. I&C experts have to be able to fulfil the requirements from HF experts. In the same manner, some I&C requirements have deep impacts on HF aspects of the HSI. For example, to ensure reasonable cost, the I&C platform can limit the number of screens that can be used in the MCR. Thus, HF experts will have to cope with this limit. Since the style guide may impact I&C platform development and may not be able to go into details without information regarding what the I&C platform and I&C detail design will look like, the style guide has to be kept as a living document and periodically developed in further detail, incorporating I&C platform progress as well as HSI/HFE design progress. In a modification project, the style guide already exists and is configured with an existing HSI design platform so that the existing style guide is a good foundation to probe which area of the HSI is likely to be impacted and needs to be considered from HFE aspects in accordance with intended HSI changes.

A.2. HUMAN ERROR PREVENTION PRINCIPLES

To prevent human error, seven principles and methods have been identified, as discussed later in this section. They are based on an analysis of standards and guidelines and they also take best practices into account.

(1) Management of human attention

This principle establishes tools that support operators to capture the necessary information in a timely manner and results in a significant reduction of the time required to locate the HSI component needed. The application of this principle reduces the potential for errors of omission, untimely execution and incorrectly selected user action during all the phases of task performance. Management of human attention is made possible by employing different information presentation methods that enhance the

original signal (flashing, animation, etc.), display a visual signal (high brightness or colour contrast), use sound (high tone or volume contrast) and use specially arranged HSI layouts.

(2) Information presentation methods

Using different and sometimes multiple and diverse information presentation methods can improve operator situational awareness by enhancing existing information. This can improve the reliability of human actions by ensuring critical information is made obvious to an operator. Examples of multiple diverse information presentation methods can be the use of colour and flashing techniques to indicate an alarm on a soft or hard control panel. Other examples can be the use of space and boundaries to relate objects (objects that are close together appear related) or the use of both visual and audible methods to annunciate an alarm.

(3) Feedback

Feedback is the method by which the operator is informed about system information. It can take many forms and can be visual (text, colour, flash), audible (alarm) or tactile (push-button, switch click). The operator can also provide feedback to the system; it is important to ensure that confirmation of an operator executed action is accurate, perceptible and timely. Feedback needs to be intuitive, that is, it needs to conform to operator expectations (e.g. clicking the left mouse button would actuate a soft control on a display screen).

(4) Protection against unintended actions

It is important to ensure that the system is protected against unintended operator actions. It is beneficial to have a system that is forgiving and tolerant of human error and to provide operators with methods of recovery from unintended actions. Generally, such errors are caused by inattention, negligence, deficit of time, combined activity, distraction, high workload and the like. These errors have been experienced in conventional nuclear power plant control rooms. For example, the button to increase reactor power was pushed accidentally as a result of the movement of a computer keyboard. A similar accident occurred when a control button was actuated by a fallen helmet. Physical barriers, special software and hardware tools as well as organizational (procedural) methods can be used to protect against unintended actions.

(5) Locking of actions

Some actions may require some form of protection that needs to be disabled to allow the operator to initiate them. This protection could take the form of a physical lock and key or of soft controls. Locking helps to prevent unintended actions caused by distraction, haste, rashness or negligence during the implementation phase of task performance. Care needs to be taken, however, that actions that may require a quick response from the operator are not unintentionally too difficult to trigger, which could increase the response time unnecessarily.

(6) Population stereotype

Operators from different countries and cultures will have different expectations for how a system performs and how feedback is given and received. This is often termed as perceived affordances. For example, the colour red may have different meanings in different cultures and so it is important to consider the cultural stereotypes for how the system interaction may be perceived. Another example of perceived affordances is that some populations write and read text from the top of the page from left to right, others

from the top but from right to left. Identifying these affordances is important to help ensure that human error potential is reduced.

(7) Supporting the operator with help and assistance

This universal principle aims to prevent all kinds of error. Through the use of various operator support systems, a wide range of tools is provided, which assist operators at all phases of performing a task.

Computerized procedures, which aim at the prevention of certain kinds of operator error during the phases of decision making, implementation and monitoring of the results are one example.

A.3. SUPPLEMENTAL INFORMATION ON WORK ENVIRONMENT CONSIDERATIONS FOR I&C

A.3.1. Lighting

The design of lighting in control rooms and related workplaces may lead to positive or negative effects on the usability of HSIs. For instance, light intensity levels that deviate from the standard threshold values can greatly impact the performance of plant staff, resulting in fatigue, stress and boredom.

In control rooms, operators are highly dependent on visual information to interact with I&C systems in all modes of plant operation. HFE guidelines state the requirement that in case normal lighting fails, an emergency lighting system has to be automatically activated and immediately available to aid the operators in performing their required tasks.

Shadows, glare, intensity, colour, contrast and location are main lighting factors that can affect the HSI of I&C equipment. Moreover, lighting can also have an influence on the surveillance and maintenance activities of I&C systems/equipment. Therefore, HFE guidelines state the requirement that those I&C cabinets that need regular maintenance inside an enclosure contain permanent lighting arrangements. If personnel have to arrange for temporary lighting at every maintenance, diagnostic, repair and troubleshooting activity, it can create an additional burden for them.

HFE and I&C engineers can consult NUREG-0700 (Rev. 2) [8], IEC 60964 [30] and ISO 11064-6 [31] as reference for design values of lighting systems. These documents contain a detailed analysis of how lighting systems should be installed in various conditions.

A.3.2. Noise

The term ‘noise’ refers to sound that bears no informational relationship to the operator. Just like light, noise level can also negatively impact human performance. An increase in the noise level in control rooms can result in permanent stress for the operators.

If noise levels are higher than a certain tolerance level, the operators need to speak louder in order to communicate with each other. Therefore, HFE guidelines recommend limiting the noise levels in control rooms within the tolerance levels of humans. During the HFE design process of nuclear power plants, a comprehensive noise evaluation is performed to recommend the estimated noise levels. However, actual noise levels can only be measured during the full functionality of the plant.

The estimated noise level value set for control rooms is very useful for the I&C engineers at the initial design and procurement stages. Based on this value set, the I&C engineers can select the rated equipment to minimize the noise level (for example, low noise level cooling fans can be selected to avoid excessive noise levels).

Several guidelines, such as NUREG-0700 (Rev. 2) [8], IEC 60964 [30] and ISO 11064-6 [31], can be consulted as reference documents for the design values of noise levels in control rooms and other related workplaces.

A.3.3. Vibration

Vibration is one of the main workplace environment factors that may affect human performance as well as the usability, operation and life of I&C equipment. In an environment with excessive vibration, operators may find it difficult to perform their intended functions. For instance, it is troublesome to acquire information from a vibrating display device or to take a reading from I&C equipment installed inside a vibrating cabinet. HFE guidelines require that workstations and workplaces be designed with acceptable limits of vibration levels.

At the initial design stage, the HFE guidelines provide a comprehensive analysis for the I&C engineers to cope with vibration levels. The guidelines recommend either procuring equipment with a high tolerance for vibrations or providing options to relocate the I&C equipment to places with acceptable limits of vibration. NUREG-0700 (Rev. 2) [8] may be used as a reference document for vibration level design.

A.3.4. Thermal environment

The appropriate thermal environment (e.g. temperature, humidity) is important for plant staff as well as I&C systems. Any change in temperature or humidity levels outside the acceptable limits may have a negative impact on human performance as well as on the life of the I&C equipment.

The thermal environment experienced by an operator can have an effect on the usability of I&C equipment. For example, extremes in the thermal environment can reduce an operator's cognitive and physical performance, affecting their ability to interact with I&C equipment.

During the initial stage of the design process, the I&C engineers need to have a detailed overview and analysis of the thermal conditions during the full operation of the plant. Based on this analysis, the designers can later procure I&C equipment that is qualified for harsh thermal environments, or will need to relocate the equipment in case thermal conditions reach their threshold ratings. Comprehensive design details are provided in guideline documents such as NUREG-0700 (Rev. 2) [8] and ISO 11064-6 [31].

A.4. GUIDANCE ON ALLOCATION OF FUNCTIONS TO HUMAN, AUTOMATION OR BOTH

Most of a nuclear power plant's control operations are routine, relatively simple and well structured. Such control tasks can be easily managed by computers. Moreover, the recent development of artificial intelligence technologies has resulted in an increase of computer capacity to handle missing data and solve poorly formalized tasks. This encourages designers to increase the level of automation as much as possible. Today, more and more control functions pass from human to automation.

However, too high a level of automation can create new and unexpected problems. The human operator remains outside of the control loop for a long time and, therefore, only observes the process and supervises the automation. Problems arise when the automation fails to manage a complicated situation. In this case, the human has to detect the failure or inadequate operation of the automation and promptly intervene in the control process. However, there is a risk that the human will not be able to cope due to being outside of the control loop for so long, resulting in a loss of skills and situational awareness distraction.

The most reasonable solution is to allocate functions so that, on the one hand, it relieves the human of tedious exhausting work, but, on the other hand, leaves some functions that ensure skill retention and permanent situational awareness.

In cases when the allocation of functions to automation is impossible or unreasonable, a harmonization of human tasks and automation can be organized in which the task to be performed manually is supported by automation. These are the kinds of automatic action that could support the human operator in the manual execution of control tasks, namely automatic identification of situations, human attention interruption and drawing attention (various kinds of alarms or notifications), performing logical reasoning and calculations, representing information to support cognitive activities, supervising human actions and detecting human errors. Cooperative work, as an example, demonstrates that allocation of functions is not a simple binary choice (i.e. manual and automatic, see Table 2).

TABLE 2. ALLOCATION OF FUNCTIONS AND ORGANIZATION OF COOPERATIVE WORK

Characteristic of control function	Assignment to		Support of human operator in cooperatively performed tasks
	humans	automation	
Workload (cumulative workload, momentary workload, psychological tension)	Low, moderate	Very low, high	Attract human attention to avoid them missing important information caused by high workload or loss of concentration
Accuracy (accuracy of spatial gestures, accuracy of estimation, timeliness)	Low, moderate	High	Supervision over accuracy and timeliness of human actions
Repetition (repetition of the same task, risk of monotony, loss of concentration)	Low, moderate	Very low, high	Supervision over human reactions and detection of human errors
Rate (rate of transient)	Moderate	High, very low	Direct human attention to the most important information and events
Available time (available time for identification of situation, available time before response action must be undertaken, available time for task performance)	Long, moderate	Little, very long	Automatic identification of a situation, direct human attention to the most important information and events
Complexity (amount of information, number of well structured logical and/or arithmetic operations)	Simple, moderate	Complicated	Performance of logical reasoning and calculations, representation of information to support cognitive activity
Consequences (impact of the task on nuclear power plant safety and efficiency)	Low, medium	High	Detection of human errors
Structurization and algorithmization of control functions	Impossible	Possible	Representation of information to support cognitive activity

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Factors Engineering in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-51, IAEA, Vienna (2019).

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

[4] 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).

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

[6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Systems and Software Engineering — Life Cycle Processes — Requirements Engineering, Standard 29148, ISO/IEC/IEEE, Geneva (2018).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[8] NUCLEAR REGULATORY COMMISSION, Human–System Interface Design Review Guidelines, NUREG-0700 (Rev. 2), Office of Nuclear Regulatory Research, Washington, DC (2002).

[9] ELECTRIC POWER RESEARCH INSTITUTE, Human Factors Guidance for Control Room and Digital Human–System Interface Design and Modification, 3002004310, EPRI, Palo Alto, CA (2015).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Automation and Humans in Nuclear Power Plants, IAEA-TECDOC-668, IAEA, Vienna (1992).

[11] ELECTRIC POWER RESEARCH INSTITUTE, Guidance for the Design and Use of Automation in Nuclear Power Plants, 1011851, EPRI, Palo Alto, CA (2005).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

[13] NUCLEAR REGULATORY COMMISSION, Guidance for the Review of Changes to Human Actions, NUREG-1764 (Rev. 1), Office of Nuclear Regulatory Research, Washington, DC (2007).

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomics of Human–System Interaction — Part 210: Human-centred Design for Interactive Systems, ISO 9241-210:2010, ISO, Geneva (2010).

[15] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE Standard 1023-2004, IEEE, New York (2005).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.27, IAEA, Vienna (2018).

[18] INTERNATIONAL SOCIETY OF AUTOMATION, Management of Alarm Systems for the Process Industries, ANSI/ISA 18.2-2016, ISA, Research Triangle Park, NC (2016).

[19] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Management of Alarm Systems for the Process Industries, IEC Standard 62682, IEC, Geneva (2014).

[20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Basic and Safety Principles for Man–Machine Interface, Marking and Identification — Actuating Principles, IEC Standard 60447, IEC, Geneva (2004).

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Computer-based Procedures, IEC Standard 62646, IEC, Geneva (2016).

[22] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE Standard 1786-2011, IEEE, New York (2011).

[23] 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).

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Challenges and Approaches for Selecting, Assessing and

Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications, IAEA Nuclear Energy Series No. NR-T-3.31, IAEA, Vienna (2020).
[25] NUCLEAR REGULATORY COMMISSION, Human Factors Engineering Program Review Model, NUREG-0711 (Rev. 3), Office of Nuclear Regulatory Research, Washington, DC (2012).
[26] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomics of Human–System Interaction, ISO 9241 Series, ISO, Geneva (since 2006).
[27] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres, ISO 11064 Series, ISO, Geneva (since 2000).
[28] DEPARTMENT OF DEFENSE, Handbook for Human Engineering Design Guidelines, MIL-HDBK-759C, DoD, Washington, DC (1995).
[29] DEPARTMENT OF DEFENCE, Human Engineering, Defense Design Criteria Standard MIL-STD-1472G, DoD, Washington, DC (2012).
[30] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Design, IEC Standard 60964:2018, IEC, Geneva (2018).
[31] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Ergonomic Design of Control Centres — Part 6: Environmental Requirements for Control Centres, ISO 11064-6:2005, ISO, Geneva (2005).

Annex I

HUMAN–SYSTEM INTERFACE INDUCED COGNITIVE ERROR ANALYSIS AND COGNITIVE WORKLOAD DISTRACTION ANALYSIS IN CONTROL ROOM DESIGN

I–1. HUMAN-–SYSTEM INTERFACE INDUCED COGNITIVE ERROR ANALYSIS

As a part of the user interface designs, especially for the control room design, human error analysis needs to be conducted in order to identify the potential for cognitive errors and to feed this information back into the design process. In cases where human–computer interaction takes place, the potential sources of cognitive errors may increase due to inappropriate user interface design (e.g. navigation functions). The interfaces could have underlying mechanisms resulting in cognitive errors that are difficult to identify or predict on the user interface.

Recently, modern nuclear power plants have widely introduced digital instrumentation and control (I&C) systems. The main human–system interfaces (HSIs), particularly those used in normal operations and design basis events, are thus largely made up of digital HSIs. The intent is to ensure that operators do not need to undertake extensive diagnostic efforts to find out the nature of an issue, but can instead rely on alarms and/or indicators to be prescribed for operator response.

It is therefore essential that the HSI design supports such a design principle by providing clear, timely, accessible and understandable information. If it is not sufficient, operators may be forced into carrying a higher cognitive burden that would cause inappropriate fault responses or a response of confused inaction, which are typical HSI induced cognitive errors.

These cognitive errors might be likely to occur in human–computer interfaces due to any of the following aspects of the HSI design:

— System and display screen hierarchy;
— Navigation features and methods;
— Graphic representation of symbols that are used for information or control on the screen;
— Layout of the symbols on the screen;
— Methods of screen based control.

In general, the underlying mechanisms resulting in cognitive errors, by their nature, are not easy to identify or predict because they result from internalized, potentially complex and interacting perceptual and psychological functions. To some extent, the outward manifestation of such errors, such as carrying out an incorrect action or refraining from action when the action is required, may be observed, predicted and quantified.

Also, in general, identifying typical human errors and using human error analysis techniques may predict where cognitive errors could occur. However, this does not necessarily clearly indicate that such manifestations are the result of cognitive errors from design and how the design may be changed to address them.

The cognitive errors themselves are not observable and are unknown even to the individual making the error; therefore, a different type of qualitative error analysis needs to be considered, one that takes into account the internal error mechanisms resulting from the perception of information and its processing through the HSI.

There is a predictive cognitive error analysis method for the HSI design, which could be applied in the early design stage to initially identify potential sources of cognitive errors within the HSI design. The method provides a structured analysis process, using systematic taxonomies that build on an understanding

of the potential cognitive errors. The applied error taxonomy includes the following cognitive aspects, each of which contains specific internal error mechanisms:

— Perception;
— Memory;
— Judgement;
— Action.

The error taxonomy is applied to the tabular task analysis already performed through the typical human error identification and human error analysis for the fault studies. The intent is to build upon the tabular task analysis structure, replacing potential error mechanisms with cognitive specific errors, and apply an appropriate set of performance shaping factors as shown below:

— Workload and distraction;
— Time pressure;
— Complexity;
— Communication;
— Environment;
— Workstation and HSI design;
— Team dynamics.

The application of predictive cognitive error analysis along with tabular task analysis provides more understanding of cognitive errors relevant to the HSI design by helping to identify the following:

— Different types of cognitive error;
— The types of cognitive aspect that are affected;
— The types of internal error mechanism that occur.

Further analysis can be considered subsequent to the predictive cognitive error analysis described above, as the results obtained can be used for further targeted analyses.

I–2. COGNITIVE WORKLOAD AND DISTRACTION ANALYSIS IN CONTROL ROOM DESIGN

In the I&C design, especially HSI design in the control room, cognitive workload and distraction analysis can be considered appropriately in order to reduce human errors. In this context the cognitive workload is considered to be any mental effort by the control room operators to meet any demands (e.g. perception, use of memory, decision making required) during plant operation. A distraction is considered to be anything that disrupts operators' attention and affects their understanding and situation awareness of the status of the plant and/or a system. The outputs from the cognitive workload and distraction analysis undertaken even in the early stage of the control room design can help inform potential design improvements and provide any findings that inform organizational measures.

I–2.1. Predictive cognitive workload analysis

I–2.1.1. Identification of candidate scenarios

A number of candidate scenarios (i.e. a task (or set of tasks) and the conditions in which it occurs) need to be identified for predictive cognitive workload analysis. This is done by discussion using suitable

prompting from the human factors engineering (HFE) team regarding likely features of high cognitive workload situations. Using this method, the following are identified:

— Distraction scenarios during routine operations that could impose a high cognitive workload on the task performer or that require the main control room (MCR) personnel to adapt a completely different mindset to carry it out.
— Post-initiating event operations that could impose a high cognitive workload due to:
  • Time pressure;
  • Complexity;
  • Concurrent processing requirements;
  • Stress or emotional state arising from the task or plant condition;
  • Perceptual difficulties caused by the design and presentation of interfaces.

I–2.1.2. Conducting task analysis

The selected scenarios include tasks that are:

— Either identified within the existing human reliability analysis (HRA) as potentially imposing a high cognitive workload on the operators;
— Or are post-fault operations identified as having the same or greater potential for high cognitive workload but not included in the HRA identified scenarios.

For the first case, detailed tabular task analyses could be used; some insights may have already been captured into cognitive workload issues. These analyses are enhanced where necessary to include more cognitive elements in the appropriate task steps and to capture the impact on any competing activities that might also need to be undertaken at the same time.

For the second case, proportionate task analysis is conducted for each task, focusing on the key steps that have cognitive elements. This is done at a high level using the hazards and operability study type method with a list of keywords and prompts to identify the cognitive elements prepared by the HFE specialist.

I–2.1.3. Applying a predictive analysis method to selected scenarios

The analysis is conducted using a workshop method with the following objectives:

— Discussing the scenarios generally to ensure that all workshop attendees thoroughly understand them, capturing any assumptions that need to be made to define a task and/or scenario well enough to analyse it and to identify any initial insights the HFE specialists have developed prior to the reminder of the task talk through;
— Identifying within the scenario the specific steps potentially requiring above average cognitive effort;
— Talking or walking through the highly cognitive task steps and rating them using established methods;
— Conducting broad but structured discussions to explore why a task (or task steps) is considered to require significant cognitive effort, using prompts to ensure that other important aspects of cognitive workload are also considered;
— Determining if the cognitive effort in each of the tasks is tolerable in the scenario modelled;
— Identifying possible solutions for reducing cognitive load for any scenarios in which the workload is not considered tolerable.

I–2.2. Predictive distraction analysis

A distraction analysis can be conducted based on the intended/planned operational practices that are usually described in the concept of operations, in which the organization of core and non-core operational tasks is described. The assignment of non-operational tasks and other activities that might be considered distracting during routine operations in the MCR are reviewed by the relevant experts, HFE teams, operations and maintenance staff. Typical review activities include the following:

— Identifying sources of potential distraction during routine operations, including non-core operations tasks.
— Defining the nature of the potential distraction, such as:
    - How MCR personnel are impacted;
    - What area of operations is affected;
    - How the distraction will be prevented or mitigated.
— Assessing any assumed or known measures for handling distractions.
— Determining the estimated impact of the expected distractions on normal plant operations. Typical points are:
    - The proportion of attention that will be taken by identified distractions;
    - Whether identified distractions can be readily and safely abandoned or suspended;
    - Whether situation awareness can be maintained or regained sufficiently rapidly.

Annex II

SUPPLEMENTAL CONSIDERATIONS FOR DIGITAL HUMAN–SYSTEM INTERFACE DESIGN

II–1. CATEGORIZATION AND GROUPING OF HUMAN–SYSTEM INTERFACE COMPONENTS

Categorization and grouping of human–system interface (HSI) components facilitate the search for information required in cases when the operator knows what information he/she needs. A few ways to group controls and displays can be used:

— *Grouping controls and displays in accordance with their belonging to a particular process system.* For example, displays and controls for the condensate system may be concentrated at the same desk, panel, visual display unit (VDU) or mimic diagram, while the components belonging to the feedwater system are located in an adjoining area or diagram.
— *Grouping displays in accordance with the category and importance of information.* For example, the most important alarm tiles reflecting safety related events are located at the top of panels, below these non-critical alarms are located, followed by gauges, recorders and relevant controls at the bottom of the panel. Alternatively, general plant overview displays may be located in an area of the control room where information may be seen by all operators simultaneously, while localized system control screens are typically only visible by the operator performing that control action.
— *Grouping information in accordance with the task performed by the operator.* Reduction/increase of power is a typical routine task of the operator. The displays and controls relevant to this task and required for performing necessary actions are concentrated on the same VDU (which may be considered a ‘task based display’) or on the same panel.

II–2. THE USE OF MIMIC DIAGRAMS

The use of mimic diagrams consists of mapping indications and controls onto a diagram of the process (e.g. a process flow diagram). A mimic diagram usually needs to be consistent with an operator’s mental model to facilitate the search of required information and to reduce the probability of confusion when perceiving data. Due to the representation of technological relationships (e.g. pipelines and electric cables connecting process equipment), mimic diagrams support the operator to foresee how particular events can affect the system. Such an approach can be applied for both conventional panels/desks and VDU based interfaces.

II–3. FORMATION AND REPRESENTATION OF GENERALIZED INFORMATION

Formation and representation of generalized information consists of combining a few items of information into one index that reflects the state of the function or the state of the process within a particular system, functional domain or nuclear power plant as a whole.

Figure II–1 illustrates the generalization of a few items of process equipment into a single mimic symbol. On the left, parallel pumps are represented as a single symbol indicating the number of pumps currently active. On the right, the turbine, the generator and their oil systems are represented by single symbols, which can change colour when some undesired event occurs within the system.

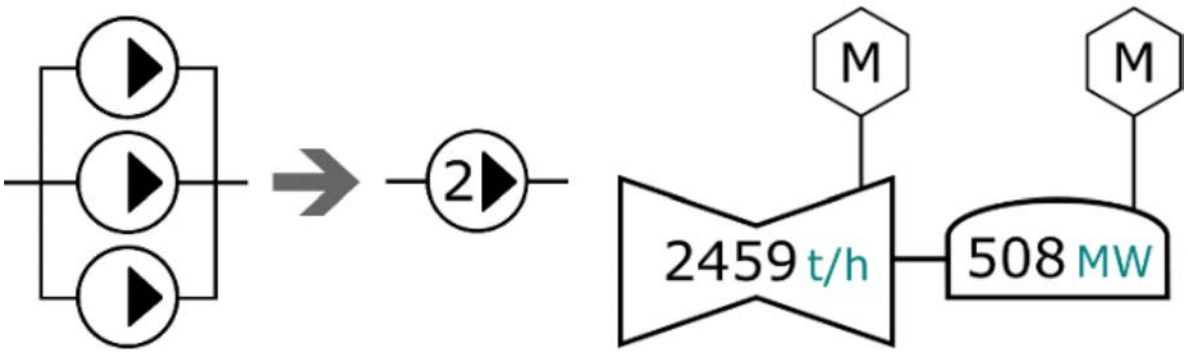


FIG. II–1. The methods of generalized representation of the equipment state.

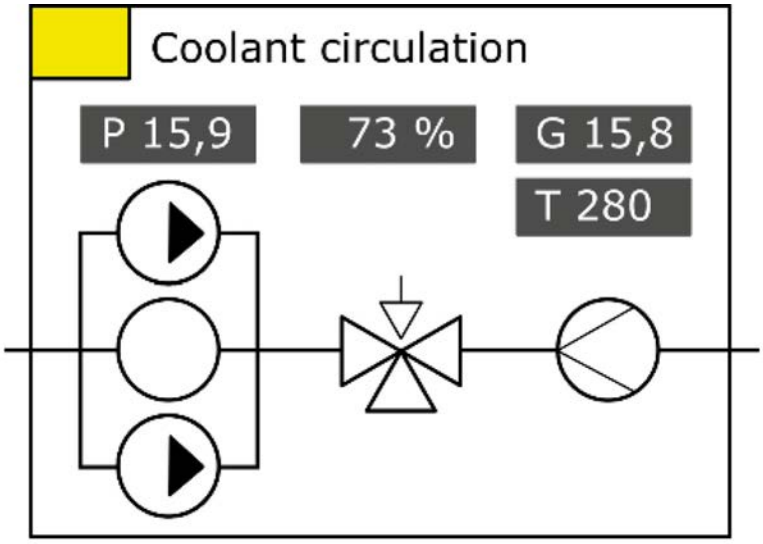


FIG. II–2. Generalization of the coolant circulation function.

A second generalization method consists of combining information into an index to support the operator in evaluation of a process function state. A typical example of an implementation of this approach is the indication of critical safety functions. The generalized index is a result of mathematical treatment and logical processing of a few process parameters and information on the equipment state. Such indication supports the operators in early detection of disturbances or the conditions fraught with deviations. Figure II–2 demonstrates an example of a functional oriented display. The function of coolant circulation is performed by three pumps and one recirculation valve. The function is in normal state when the coolant pressure is 15–17 MPa, the coolant flow rate is 15–18 t/s, two pumps are active and one pump is in standby mode. As shown in Fig. II–2, all the process parameters are within acceptable limits; however, one pump is out of service instead of standby mode. This means that the function is under threat and its status is indicated by the yellow marker.

When representing generalized information, it is very important to provide operators with the possibility to look at the algorithm used to calculate the generalized index (e.g. the logical tree, decision table). The operator needs to have transparency in the logic behind the representation.

II–4. REPRESENTATION OF OVERVIEW INFORMATION

A plant overview display is a VDU format in which generalized information is mapped onto a structural diagram of the whole nuclear power plant to indicate the overall plant status. The level of plant structure realized in the overview display may vary considerably from detailed representations to high level, simplified representations. An overview display is a combination of the previous two approaches, the representation of generalized information and the use of mimic diagrams. The overview display performs three tasks:

(1) It allows the operator to evaluate the status of the nuclear power plant as a whole, as well as to see the current configuration of the equipment and the most important parameters at a glance.
(2) It supports the operators responsible for a particular functional domain (e.g. reactor, turbine, auxiliary systems) to maintain awareness of the status of the rest of the station. This allows them to plan their control actions, taking into account the overall conditions at the nuclear power plant.
(3) It provides a common situation awareness and common information space for effective communication among several control room operators.

There are three categories of overview display:

(1) Shared overview displays for the representation of the main process parameters and recent configuration of the nuclear power plant equipment;
(2) Personal overview displays for the representation of generalized status (or generalized alarm) of process systems or process functions relevant to a particular operator's activities;
(3) Personal or shared overview displays for the visualization of material and energy balances around the nuclear power plant.

The information content may vary from plant level overviews to system level overviews to control function overviews. As a rule, the first category of overview display looks like a generalized mimic diagram representing one power unit or the nuclear power plant as a whole together with the main process parameters mapped onto the diagram. The main task to be solved during the design of such an overview display is to select the most important information for representation to operators. The following criteria need to be considered to support design decision making:

— Whether the information is relevant to the safety and efficiency of the process;
— Whether the information is significant for understanding the material and energy balances within the nuclear power plant.

This type of overview display is usually displayed on a wall mounted large screen display (video wall), which is readable and perceivable by all control room operators. An example of an overview display is shown in Fig. II–3.

The second type of overview display is intended for the representation of generalized information on the state of the process systems or the process functions belonging to the area of responsibility of the operator. The generalized information on the operation of a process system can be represented without mapping onto a generalized mimic diagram; however, it is reasonable to group the systems into functional domains to support the perception process (see, for example, Fig. II–4).

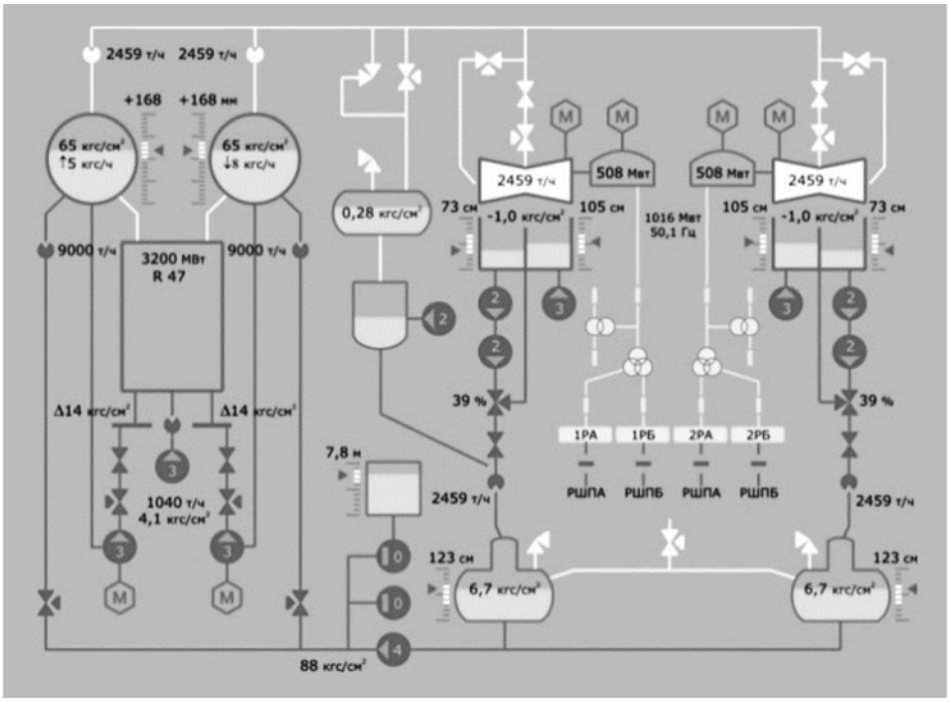


FIG. II–3. Overview display for representation of the main process parameters and recent configuration of the nuclear power plant equipment.

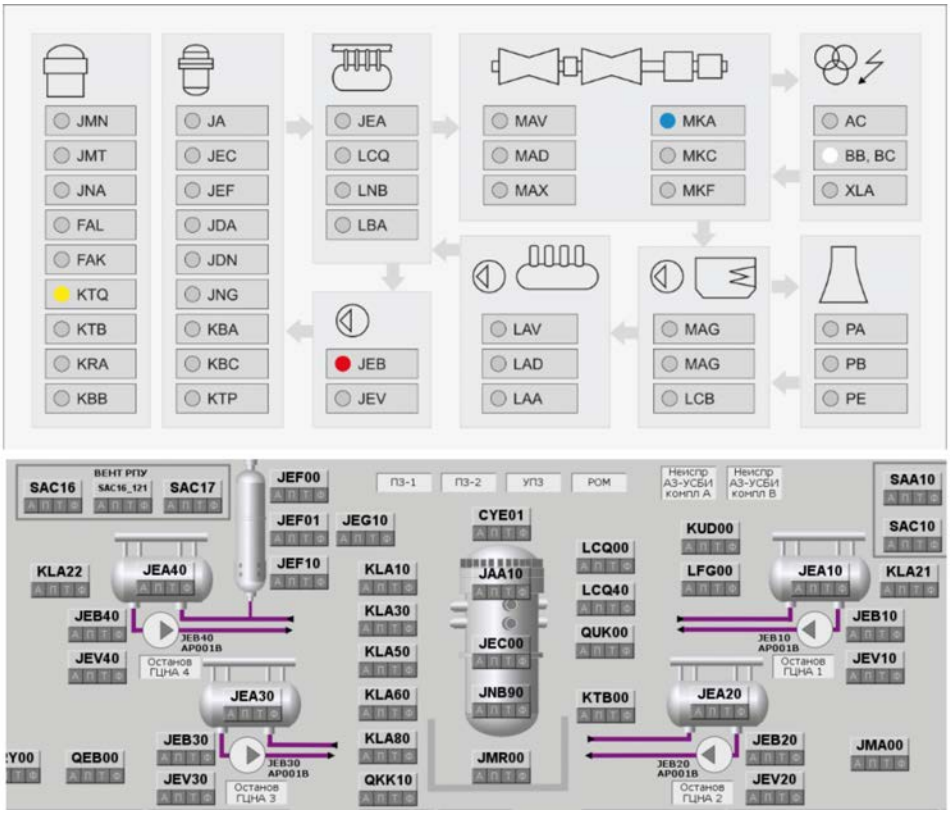


FIG. II–4. Simplified overview displays for the representation of generalized alarms and quick call of the required VDU area.

This type of overview display can be used as an operator menu facilitating navigation and selection of the required VDU information representing the system where undesired events (alarms) have occurred. As a rule, such overview displays are visualized at one of the screens of the operator's workstation.

The third category of overview display is intended to indicate the state of material and energy balances in the nuclear power plant. The energy balance can be affected by events such as failure to remove heat, underheating of medium (i.e. water, gas or air), inadequate generation of electricity for internal consumers, inadequate consumption of produced electricity and so on. A reduction of medium flow due to a leak or an increase or decrease of demands for the quantity of the medium can affect the material balance. Material or energy imbalance can lead first to a local disturbance (for example, rise of temperature, pressure drop or fall of level) and then to a global change of the nuclear power plant mode. In such a case, it is important to ensure that operators are aware of the available reserve of energy and/or medium.

II–5. ECOLOGICAL APPROACH TO VISUALIZATION OF INFORMATION

When assessing the situation, operators have to perform many cognitive operations, such as arithmetic operations (e.g. addition and subtraction), comparison and evaluation of differences between values (including analogue or discrete values), making logical conclusions using the 'if-then' rules, and so on. On their face, these operations are quite simple; however, their execution becomes significantly slower under stress conditions accompanied with a time deficiency. Reducing the cognitive load is made possible by transferring these operations from the level of logical thinking to the level of perception (scientific publications may mention this approach as 'visual thinking').

The visual thinking phenomenon is illustrated in Fig. II–5.

The Figure contains two analogue meters displaying two water flow rates on the left and two boxes with digital parameters typical for a computerized interface on the right. The following information can be easily revealed from the analogue instruments without any calculations: (1) there is a difference between two flow rates, (2) the upper flow rate is much less than the lower one, (3) the value of the upper flow rate is close to the alarm set point (it needs to be noted, that the information in (1) and (2) is essential only if the task to be performed by the operator involves comparison of these two parameters). To extract this information from the digital boxes shown to the right, the operator has to perceive and interpret two numerical values, mentally compare them, calculate the difference, recall the set point from memory and compare the values with this set point. This example does not prove that the analogue meter is definitely better than the digital one. However, unlike the digital indication, the analogue meter forms a visual image, which helps the operator to quickly understand the situation. The HSI based on such images is often mentioned in the literature as an 'ecological interface', 'cognitive graphics', 'high performance interface', 'analytical interface' and so on.

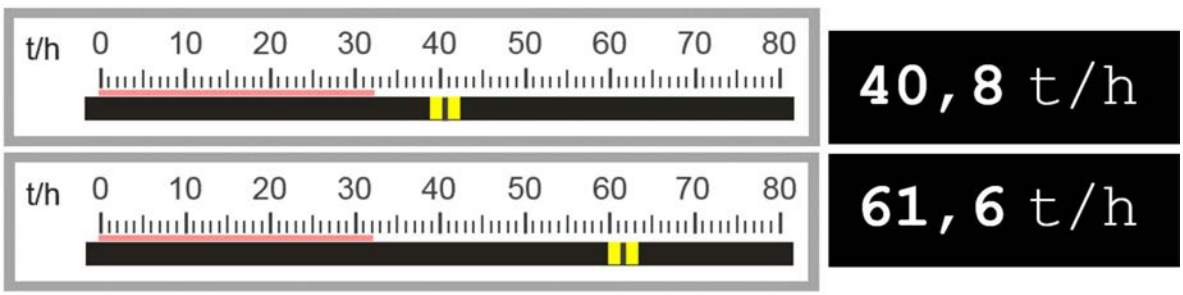


FIG. II–5. Representation of parameters using analogue instruments and digital boxes.

The graphical patterns used to transfer mental operations to the level of perception are shown in Fig. II–6. The most frequently used way to display the value of an analogue parameter is a bar chart with a horizontal or vertical scale, but other methods, such as circular or semicircular scales, pie charts and the like can also be used.

To visualize the operation of addition or subtraction, a segmented bar consisting of two or more bars superimposed on each other can be used (as shown in Fig. II–6a). The operation of subtraction has a specific feature: the bar cannot be shortened (as done in Fig. II–6b) if there is a set point associated with the displayed parameter. In this case, the subtraction operation is visualized by shifting the scale in the corresponding direction (as shown in Fig. II–6c).

To visualize the prediction of the parameter change, an additional pointer can be used (see Fig. II–6d). This pointer indicates the value that, as supposed, will be reached by the parameter in some predetermined time. The time needs to be preliminarily chosen and fixed, taking into account the quickness of the transient processes.

The visualization of the operation of comparison between two parameters is shown in Fig. II–6e (detailed and simplified view). Such a method of visualization is very effective when monitoring the balance between two or more parameters. If these parameters have different scales, they can be scaled so that the bars have the same length when the balance is reached.

The comparison of several parameters with each other may be required not only to estimate the balance, but also to monitor if the parameters are within the allowed limits. Figure II–6f shows an example of this case.

Figure II–6g demonstrates the bar chart that supports the tracking of consecutive heating of water as it is transferred from one heater to another. This task also requires the comparison of several parameters. In addition to the temperature values, the chart contains lines indicating the set points, forming a ‘corridor’ of acceptable values.

The ratio of two parameters can also be represented in the form of a phase diagram. A P-T (pressure temperature) diagram is a typical example for this kind of visualization (see Fig. II–6h). The water heating diagram and the P-T diagram can be combined as shown in Fig. II–6i. The P-T diagram superimposed on the temperature diagram shifts to the left or to the right when the pressure changes.

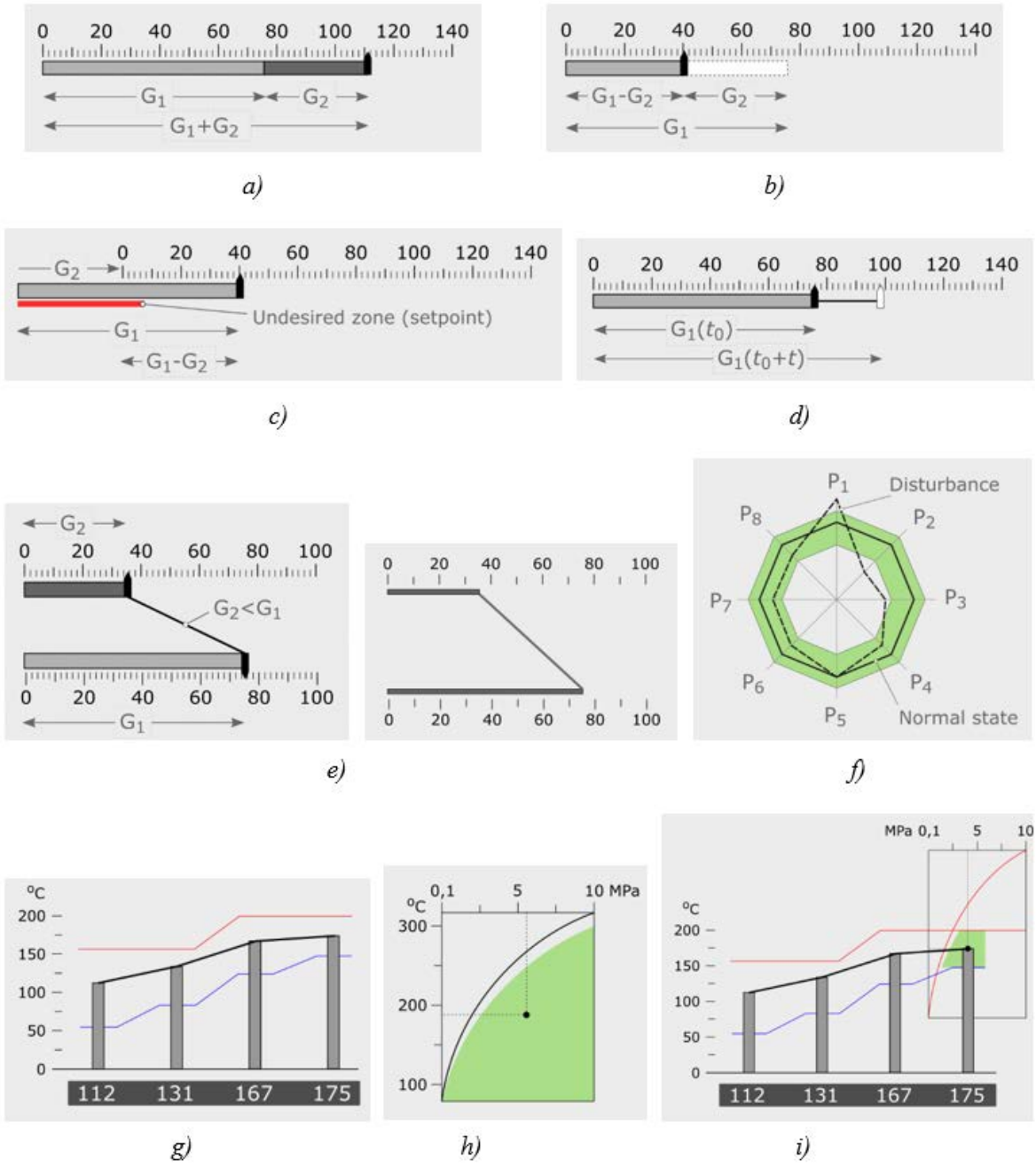


FIG. II–6. Visualization of addition (a), subtraction (b, c), prediction (d), comparison (e) and matching of several parameters (f–i).

Annex III

VERIFICATION AND VALIDATION METHODOLOGIES AND ACCEPTANCE CRITERIA

III–1. VERIFICATION METHODS

Human factors engineering (HFE) verification is aimed at examining whether all relevant requirements stated in standards, guidance, contract and other documents have been satisfied.

Usually, the subject of requirement can be measured by instruments or can be simply checked using project documentation, visual display unit (VDU) formats, control room equipment and the like. For example, a requirement such as "sound intensity should be limited to a maximum of 95 dB" can be verified using a sound level meter. Similarly, a quick glance at a desk, panel or scheme may be sufficient to verify the requirement that "the devices required for safety and normal minute to minute operation should be close to the operator's monitoring position."

The expert evaluation method can be used to verify requirements that cannot be measured or checked. For example, some requirements can refer to subjects such as a comfortable environment, easy access, good visibility, convenient location and so on. In order to estimate these, respondents (experts or potential users) can be asked to evaluate comfort, convenience, accessibility and other characteristics using quantitative or qualitative scales, such as the following:

— Nominal scale, where the respondent uses words (labels) describing his/her opinion, such as 'good', 'poor', 'nearly comfortable';
— Ordinal scale, for example, a scale from 0 to 10, where 0 means an absolutely unacceptable situation and 10 means a very good solution;
— Comparative estimation, where the respondent compares two or more subjects and evaluates them using such categories as 'better', 'much better', 'worse'.

Some additional preparation is needed to verify a requirement such as "the design should accord with accepted population (and professional) stereotypes." If the project documentation does not contain information on these stereotypes, then the person who carries out an examination of this requirement has to reveal them. This can be done by means of a structured interview.

For example, to reveal professional stereotypes in the area of coding of information, the colours, symbols, patterns and other solutions that will potentially be used can be presented to the future users of the system without providing any explanation of their meaning. The respondents are asked to describe how they interpret these colours and symbols. After comparing the answers with the designers' original intention, a conclusion can be made on the conformity of the design with user stereotypes. This method can also be used to evaluate the intuitive clarity of the selected coding principles.

To verify some requirements, a systematic view can be used. For example, in order to verify the requirement that a "code (shape, pattern or size) shall be applied to all controls throughout a particular NPP [nuclear power plant]", it would be reasonable to put all of the gathered information into one spreadsheet to facilitate the comparison (see Table III–1 for an example). It is important to involve not only human–system interface (HSI) components but also elements of interior design in the analysis.

TABLE III–1. SPREADSHEET FOR SYSTEMATIC VIEW OF CODE CONSISTENCY

Code	HSI component	Meaning
Red colour	Alarm tile	Emergency, high priority
	Control switch	Protection activation
	Sign	Prohibition

III–2. HFE HSI AREAS TO BE USED FOR DESIGN VERIFICATION

Typical areas used for design verification are those included in NUREG-0700 (Rev. 2) [III–1]:

Area 1:

General guidelines associated with design, such as consistency and feedback.

Area 2:

Guidelines associated with how information is displayed (differentiating software and hardware), considering the following areas:

— Display formats, meaning methods for arranging information such as tables, lists, mimics, diagrams, data forms and fields, maps, charts (pie, bar), graphs and virtual instrument panels;
— Display elements, meaning the parts that build a display format such as alphanumeric characters, borders, lines, arrows, abbreviations, acronyms, colours, labels, coding (by size, shape, pattern), icons, symbols, numeric data, scales, axes and grids;
— Highlighting (brightness and flashing);
— Auditory coding;
— Data quality and update rate;
— Display pages;
— Display devices.

Area 3:

Guidelines associated with user–system interaction, understanding the different ways the user can manage and introduce inputs to the system and can receive and control information (computer centred). This is conditioned by the type of HSI, addressing the following areas:

— General user input guidelines;
— User input formats (command language, menus, function keys);
— Cursors (type, appearance, controls, number);
— System response (prompts, feedback, response time);
— Managing displays (display selection, navigation, window management, display control, information update/freeze, scrolling, paging);
— Managing information (editing, saving, exporting);
— User assistance (confirmation messages, input confirmation, data protection);
— Interface flexibility;
— System security (information access and identification).

Area 4:

Guidelines associated with controls, evaluating all the controls from which the operator actuates, encompassing the following items:

— Controls for using computerized systems, such as keyboards, touch screens, light pens;
— Conventional controls, such as push-buttons, rotary controls, thumbwheels or switches (slide, toggle, rocker);
— Soft controls (virtualizing any of the conventional model).

With regard to conventional controls, there is guidance in some countries about the required dimensions, which are normally big enough for use in adverse conditions (even considering the use of gloves). (However, operational experience has also demonstrated the safe use of mini controls in mosaic panel designs, which would not comply with the minimum dimensions of available HFE guidelines.)

Area 5:

Guidelines associated with specific HSI systems such as:

— Alarm systems, considering conventional (spatially dedicated continuous visible) and advanced systems, definition, coding, user–system interactions, maintenance, layout and integration;
— Computerized procedure systems;
— Safety function and parameter monitoring systems;
— Group view display systems;
— Automation and computer operator support systems (understanding those as an aid, not essential for plant operation);
— Communication systems (speech based and computer based).

Area 6:

Guidelines associated with workstation and workplace design such as:

— Considering workstations as places where the operators perform their tasks, encompassing sit-down or stand-up panels, vertical panels, desks and others (i.e. chairs, control display integration, layout);
— Considering workplaces as places where the workstations are located (e.g. main control room (MCR), remote shutdown station, local control stations).

Other considerations include the environment in which an instrumentation and control (I&C) system is used, which can have a positive or negative impact on both the function of the I&C system and on the human interfacing that equipment. It is important to ensure that both environmental considerations and I&C are optimized to support the HSI. The following need to be addressed as a minimum:

— Lighting;
— Noise;
— Vibration;
— Thermal environment.

Area 7:

Guidelines associated with maintainability, encompassing the following items:

— I&C equipment features of digital systems;
— I&C equipment features of analogue systems;
— Area/facility features where the I&C is to be installed (to enable maintainability);
— Manuals;
— Workshops.

Area 8:

Guidelines associated with degraded HSI and I&C conditions, encompassing the following items:

— HSIs for monitoring I&C system conditions;
— HSI response to I&C system changes;
— Information sources and validity;
— Backup of HSI and I&C failures.

III–3. USE OF HFE GUIDELINE CHECKLISTS DURING VERIFICATION

The desired HFE design verification results ideally confirm that the majority of guidelines and style guide requirements are fulfilled. The following are typical possible results from this type of verification:

— Guidelines fulfilled;
— Guidelines not fulfilled but reasonably justified;
— Guidelines not applicable;
— Guidelines in discrepancy status due to a deficiency;
— Guidelines in pending status (typically of interim results).

The inclusion of the rationale for the status of each guideline is advisable for allowing traceability, subsequent review and justification of the guideline's status.

Typical HFE design verification discrepancies and deficiencies include the following:

— Discrepancies in the HSI that simply have not matched all HFE guidelines in some way within different displays or panels (e.g. inadequate/inconsistent HSI layout, inadequate/inconsistent HSI component placement or inadequate HSI component properties);
— Discrepancies in the HSI due to different design criteria (following the same HSI style guide);
— Discrepancies in the HSI when primarily based on a design specification that has no considered HFE guidelines;
— Discrepancies in the HSI after trying to address a previous discrepancy;
— Discrepancies that are outdated (when a new design revision is issued, planned or unplanned).

For hardware panels, maintainability can be compromised if the front design and layout of components do not take into account maintainability issues such as electrical train or fire zone separation.

The end goal for verification is to document and provide evidence that the design has adhered to the requirements and usability principles with regard to verification against HFE guidelines and standards.

III–4. VALIDATION METHODOLOGY

Validation is most effective when implemented throughout the HFE design process. In best practice this occurs iteratively, in which the design team is able to address and resolve issues identified during early usability testing and early validation before conducting subsequent validation activities throughout the design process. There are different types of validation and different times in the project when validations can be performed. It is generally understood that multiple validation exercises may be warranted for a project for which there is an iterative design process.

HFE validations can credit early usability testing and validations throughout the process in which the design requirement and HFE recommendations are met, so the duplication of effort does not occur on a priority and graded approach.

HFE system validation planning for modernizations and new builds can consider the following:

— A single stage approach at the end of the HFE process for a small I&C project (i.e. upgrading of a specific analogue or digital controller model due to obsolesce with a new digital controller that performs the same or similar function), commonly known as integrated system validation (ISV).
— A multistage approach, considering partial or preliminary validation stages throughout the design process prior to the final ISV (which could also be staged). Stages could consider different types of HSI (operating displays, alarm systems, procedure systems), as well as when part of them become available (lots, batches), including interim configurations in which modifications are performed through several outages.

ISV is a performance based evaluation of the integrated HSI design. The performance is measured in terms of the plant parameters, personnel tasks, crew communications and coordination, situation awareness, workload (both cognitive and physical) and anthropometric and physiological factors. The entire HSIs of the control rooms developed for the simulator are within the scope of ISV activities, including control rooms, panels and components.

ISV is also used to evaluate the acceptability of those aspects of the design that cannot be evaluated through analytical means, namely, task support verification or design verification. Deficiencies generated from task support verification or design verification are resolved during preliminary validations. Full scope simulators can be used as the test bed during ISV activities. Operational scenarios need to be predefined before ISV execution, sampling dimensions such as plant conditions, personnel tasks and situational factors that challenge personnel performance. ISV data and analysis results need to be documented in the ISV report along with all discrepancies generated from ISV. They need to be closed before the plant is placed into operation.

A multistage validation approach could have the following advantages:

— It provides results early in the design stage, when changes are easy to make.
— It provides feedback from users, or even end users, so that they are familiar with the design in advance and are thus able to make any necessary adjustments.
— It provides detailed results, stage by stage, for each HSI component to better adjust the HSI under design.
— It avoids major findings in the final ISV with important economic and scheduling consequences.
— It minimizes the possibility of an additional ISV.

Partial or preliminary validation stages normally do not have a full scope simulation available until the final ISV; consequently, only limited approaches such as walk through/talk through approaches or partial/limited dynamic capabilities are possible, providing initial and useful results. Nevertheless, efficiencies can be achieved from these early table top validations to early prototype usability testing at the ISV stage by already having addressed or evaluated design requirements at an early stage resulting in a reduced level of effort at the final ISV.

III–4.1. Methods, criteria and measures

Multistage and ISV iterative validations need to consider aspects such as planning, test methods, training, performance measures, testing criteria and data collection and analysis. This section describes best practices in execution of the methodology described in IAEA Safety Standards Series No. SSG-51, Human Factors Engineering in the Design of Nuclear Power Plants [III–2].

It may be useful to develop mock-ups or prototypes of design concepts. Mock-ups and prototypes may range from low fidelity (e.g. paper printouts of design screens) to high fidelity (e.g. functional software interfaced with a simulator). Providing examples of design products can provide the opportunity for early design validation from end users, such as operators. The examples may also allow verification of the design to applicable human factors standards. Early verification and validation can help solidify the design and prevent the need for reworking prior to implementation.

Training is required for validation teams so that team members can anticipate operator actions in each scenario and better judge the appropriateness of their actions. Participant/crew training is necessary so that the use of HSI parallels what their regular operation will be and does not result in a biased performance. Suitability analysis can be completed for each user type and fed into or confirm the validation methodology and plan.

Examples of validation issues or criteria to be tested include the following:

— Generic primary tasks performed by plant personnel (monitoring, situation assessment, response planning and response execution activities based on a human performance model);
— Secondary tasks (movements or navigation actions for accessing information);
— Workload (for particular activities or within entire scenarios, considering cognitive and physical workload);
— Situation awareness (for global scenarios);
— Teamwork;
— Communication.

Examples of performance measures for substantiating validation issues or criteria to be tested include the following:

— Time for performing actions;
— Precision;
— Accuracy;
— Frequency of actions;
— Amount achieved;
— Number of errors;
— Information exchanged (communication);
— Anthropometry/crew movements;
— Plant parameter values (along the scenario or at certain moments);
— Crew ratings for specific questions.

These performance measures will be able to substantiate (qualitatively and quantitatively) crew performance in the context of the role played in the scenario. Performance measures can be taken during an ISV by direct observation, interviews and with various means of recording. Error tolerance requirements to prevent single point failures (such as inadvertent actuation) built into the design become an important aspect of validation testing in performance measures.

Quantitative measures are not necessarily more valid than qualitative measures. Measures are selected according to those that help answer the design questions related to whether or not the system and HSI are usable by operators. A hallmark of the graded approach is the use of only the most efficient measures; different pieces of evidence may be used in the validation of the system. Validation may occur at multiple stages of the design process and each stage presents opportunities to evaluate the design. The use of both formative (design

stage) and summative (final acceptance testing) evaluation may provide evidence for an overall safety case. The outcome of the validation is documented and used as the basis for acceptance of the final design prior to implementation.

Data collection of the performance measures can be carried out with the following methods:

— Direct observations or annotations in a log: This is done by the validation team members and the log includes performance measures or annotations by which performance measures can be calculated (the latter being the most common way to produce performance measures). Information to be recorded includes replies to the following questions:
  - Who performed any actions and which actions?
  - What was the time when the actions were performed?
  - What information was used?
  - Which procedures were followed/used?
  - What information was exchanged?
  - Which HSI portion was used?

  With this log, performance measures can be derived or produced in many ways (frequency of actions, elapsed time for an activity, etc.).

— Interviews: They are preferred after scenario execution with the purpose of asking crews to summarize what happened during the scenario and also of formulating any specific questions because of special issues observed during the scenario.
— Video recordings: They are another way or backup for obtaining observations and calculating performance measures (can be time consuming).
— Simulator recordings: They are based on plant parameters during scenarios that can provide an idea of the effectiveness of operator actions in plant performance.
— Observer's ratings: They can be based on the direct observations of the observer team members or participant/crew ratings.

III–4.2. Scenarios

Validation activities consider the opportunity for user performance to affect the successful and safe use of the system. Realistic and representative use scenarios can be developed and run on a realistic version of the actual system.

The ISV test design has to consider how many scenarios are sufficient to provide enough proof of the adequate HSI design and operator training to guarantee safe operation under all conditions relevant to the design. The scenarios can be short or long or consider different plant operations in each of them. Normally the most risk-important scenarios are those that are tested more in new designs because they consider the most challenging situations for plant safety and for crews. Risk-significant or critical human actions as candidate scenarios may be identified in the human reliability analysis when available. Also, the scenarios to validate the I&C components and systems need to be relevant to the plant equipment.

Relevant plant situations that need to be considered when planning a validation include the following:

— Normal operation, such as startup, shutdown, fuel load and load change;
— Failures of individual or several I&C components, HSIs or the distributed control system (part or the entire system);
— Transients, such as turbine trip, external power loss, station blackout, feedwater loss, essential service water loss, electric busbar power loss, safety and relief valve transients;
— Accidents, including steam line breakage, positive reactivity addition, control bar insertion during full load operation, anticipated transients without scram, steam generator tube rupture and loss of coolant accidents.

The above listed scenarios may include risk-significant actions such as manual depressurization or feed and bleed activities as well as special situations related to the failure of I&C equipment. These scenarios need to be tailored for each specific plant validation as they are dependent on the technology of the plant under consideration.

The ISV test design needs to also consider the number of crews who will role play in the scenarios, as well as the sequencing of these scenarios for each crew. The following aspects need to be considered:

— The number of crews that participate in an ISV has to be representative or statistically significant;
— In order to avoid biased results due to already expected scenarios, scenario sequencing needs to be modified per crew so that they will not know in advance the scenario they will face.

III–4.3. Data analysis

Data analysis will engage in the following activities:

— Analyse individually each scenario;
— Compare the same scenario role played by each different crew;
— Compare the results of the different scenarios;
— Analyse the results according to the classes of situation as several scenarios can be instances of the same class of situation, resulting in the need to analyse results at the class level.

The depth of analysis needs to align the level of risk and validation of the design, specifically to confirm that the HFE and user design requirements are met. Deficiencies are noted as either minor, moderate or major with and the requisite means to address these:

— Major deficiencies requiring redesign;
— Moderate deficiencies requiring review of procedures and training to decide on redesign;
— Minor deficiencies requiring disposition.

As the minimum, actions are required for the disposition of deficiencies. The absence of changes needs to be justified as does the description of the changes to be performed when necessary (by the appropriate team). The need for an additional validation to check how certain discrepancies are resolved is dependent on whether the discrepancies are important based on consequence and risk.

Human performance may be assessed in a variety of ways, including qualitatively and quantitatively. Examples of qualitative measures include, but need not be limited to, the following items:

— Successful recovery from failure to complete the scenario using the HSI;
— Design recommendations such as those obtained from operator feedback;
— Fixation areas.

Validation reporting needs to consider, among others, the following aspects:

— Description of test and evaluation conditions;
— Summary of results per HSI component, per scenario and per validations item/objective;
— ISV acceptance criteria fulfilment;
— ISV general results and recommendations;
— ISV conclusions;
— ISV report appendices that support the conclusions and general results (including scenario logs, other scenario recordings, etc.).

III–5. VERIFICATION AND VALIDATION ACCEPTANCE CRITERIA

Acceptance criteria can be understood as those indicators that demonstrate that the verified and validated design complies with its intended functions.

For I&C, the development of acceptance criteria can be objective enough based on design and performance requirements. After I&C testing (such as factory testing or functional testing), the performance measures obtained can demonstrate the fulfilment of the I&C acceptance criteria. Therefore, the assessment of acceptance criteria fulfilment can be straightforward, comparing numeric measures with thresholds (based on the requirements defined) or with the existing functionalities (versus those planned) under certain plant conditions.

For HFE, the development of these acceptance criteria may not be so straightforward. In the case of verification, these acceptance criteria are easier to fulfil because it is simple to comply (or not) with HFE guidelines. In the case of validation, acceptance criteria are more difficult to develop because of human performance variability and because different performances do not necessarily mean that one is worse than another in terms of meeting plant safety and adequately fulfilling plant operation objectives.

In these HFE validations there is indeed a link with I&C because I&C is used during the applicable validation scenarios to be enacted.

Experience in developing acceptance criteria for HFE validation show approaches based on human capabilities, considering the following categories and subcategories:

— A human performance model that can include:
  - Monitoring/detection activities;
  - Situation assessment activities;
  - Response planning activities;
  - Response implementation.
— Human performance centred issues (global for the scenario) such as:
  - Situation awareness;
  - Workload;
  - Teamwork and communication.

The acceptance criteria to be developed with this approach can be sufficiently generic that they apply to all the plant conditions to be tested, or more specific, being scenario oriented. The development of scenarios for HFE validations is based on operational experience in plants and the scenarios need to include a description of plant performance together with the expectations for operators.

The analysis of fulfilment of acceptance criteria categories can be based on the adherence of the prescribed scenarios with what operators have done during the actual scenarios, documented in scenario logs with performance measures. Human error is an important performance measure, as is the time needed to complete individual tasks or the whole scenario, among other measures that have been described in previous sections within this annex. These measures can be the basis for scoring and evaluating acceptance criteria.

Although the results of evaluating acceptance criteria can be shown in many ways, the basic result to consider is whether or not these criteria (including safety and operational objectives) are met.

I&C engineers will need to consider the outcomes of HFE validation and acceptance criteria fulfilment because results can impact their design.

REFERENCES TO ANNEX III

[III–1] NUCLEAR REGULATORY COMMISSION, Human–System Interface Design Review Guidelines, NUREG-0700 (Rev. 2), Office of Nuclear Regulatory Research, Washington, DC (2002).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Factors Engineering in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-51, IAEA, Vienna (2019).

GLOSSARY

The following definitions are specific to this publication.

architecture. Organizational structure of the instrumentation and control (I&C) systems.

computer based procedures. Presentation of plant procedures in computer based rather than paper based formats to help personnel achieve the aims of the procedures.

computer security. Capability of a digital system to protect information and data so that unauthorized persons or systems cannot read or modify relevant data or perform or inhibit control actions, and authorized persons or systems are not denied access.

concept of operations in end point vision. A concept of operations describes the proposed design in terms of how it will be operated to perform its functions, which includes the various roles of personnel and how they will be organized, managed and supported. The concept of operations describes how the plant is operated ('operating philosophy') and includes aspects such as the size and composition of the operating staff and how they operate the plant under normal and abnormal conditions. (The document may also be referred to as 'a concept of operations and maintenance' to include a description of maintenance aspects of the system as well.)

end point vision. A concept for the final human–system interface (HSI) after I&C system modification has been completed. A target or vision that can be used to guide the design of modifications over time so that they work toward the desired final product.

human–system interface. The interface between personnel and instrumentation and control systems and computer systems linked with the plant. In the context of this publication, the HSI is considered an integrated part of the I&C system.

I&C architecture. The organization of the complete set of I&C systems.

I&C engineer. Any person involved in the life cycle of an I&C system or the overall I&C.

I&C system. Refers to any I&C system introduced into the design of the plant.

maintainability. The design of equipment to support effective, efficient maintenance activities.

mobile device. HSI device used by mobile workers (e.g. field operators) while they are in the field.

modernization. A project or programme that involves either implementation of new I&C systems or a significant technological upgrade of an existing I&C system.

modification. A project that involves change to an existing I&C system. This change can include modernization, but it often refers to replacement of old equipment and is limited in technological advancement.

smart device. Device (e.g. sensor, actuator control, power supply, visual display unit) that has one or more digital parts providing advanced functions and services.

style guide. A document that contains guidelines that have been tailored so they describe the implementation of human factors engineering guidance to a specific design, such as for a specific plant control room.

ABBREVIATIONS

CBP	computer based procedure
FRA	function requirements analysis
HF	human factors
HFE	human factors engineering
HRA	human reliability analysis
HSI	human–system interface
I&C	instrumentation and control
ISV	integrated system validation
MCR	main control room
OER	operating experience review
V&V	verification and validation
VDU	visual display unit

CONTRIBUTORS TO DRAFTING AND REVIEW

Adran, A.B.	Horizon Nuclear Power, United Kingdom
Anokhin, A.	Rusatom Automated Control Systems, Russian Federation
Barker, D.	Wood Group, United Kingdom
Boring, R.	Idaho National Laboratory, United States of America
Couix, S.	Électricité de France, France
de Oliveira, L.N.	Eletrobras Eletronuclear, Brazil
Duchac, A.	International Atomic Energy Agency
Eiler, J.	International Atomic Energy Agency
Ferreira, E.	Bruce Power, Canada
Kiani, I.B.	Pakistan Nuclear Regulatory Authority, Pakistan
Kim, J.T.	Korea Institute of Nuclear Safety, Republic of Korea
Kim, S.K.	Korea Atomic Energy Research Institute, Republic of Korea
Loughrey, M.	Point Lepreau Generating Station, Canada
Mashio, K.	Mitsubishi Heavy Industries, Japan
Mbonjo, H.	GRS GmbH, Germany
Naser, J.	Consultant, United States of America
Ngo, C.	Kinectrics Inc., Canada
Nguyen, T.	Électricité de France, France
Savioja-Kangasluoma, P.	STUK — Radiation and Nuclear Safety Authority, Finland
Screeton, R.	Office for Nuclear Regulation, United Kingdom
Stewart, A.	Canadian Nuclear Safety Commission, Canada
Tominaga, K.	Hitachi–GE Nuclear Energy, Japan
Trueba, P.	Tecnatom, Spain
Wang, Y.	China Nuclear Power Engineering, China
Yu, G.	China Nuclear Power Engineering, China

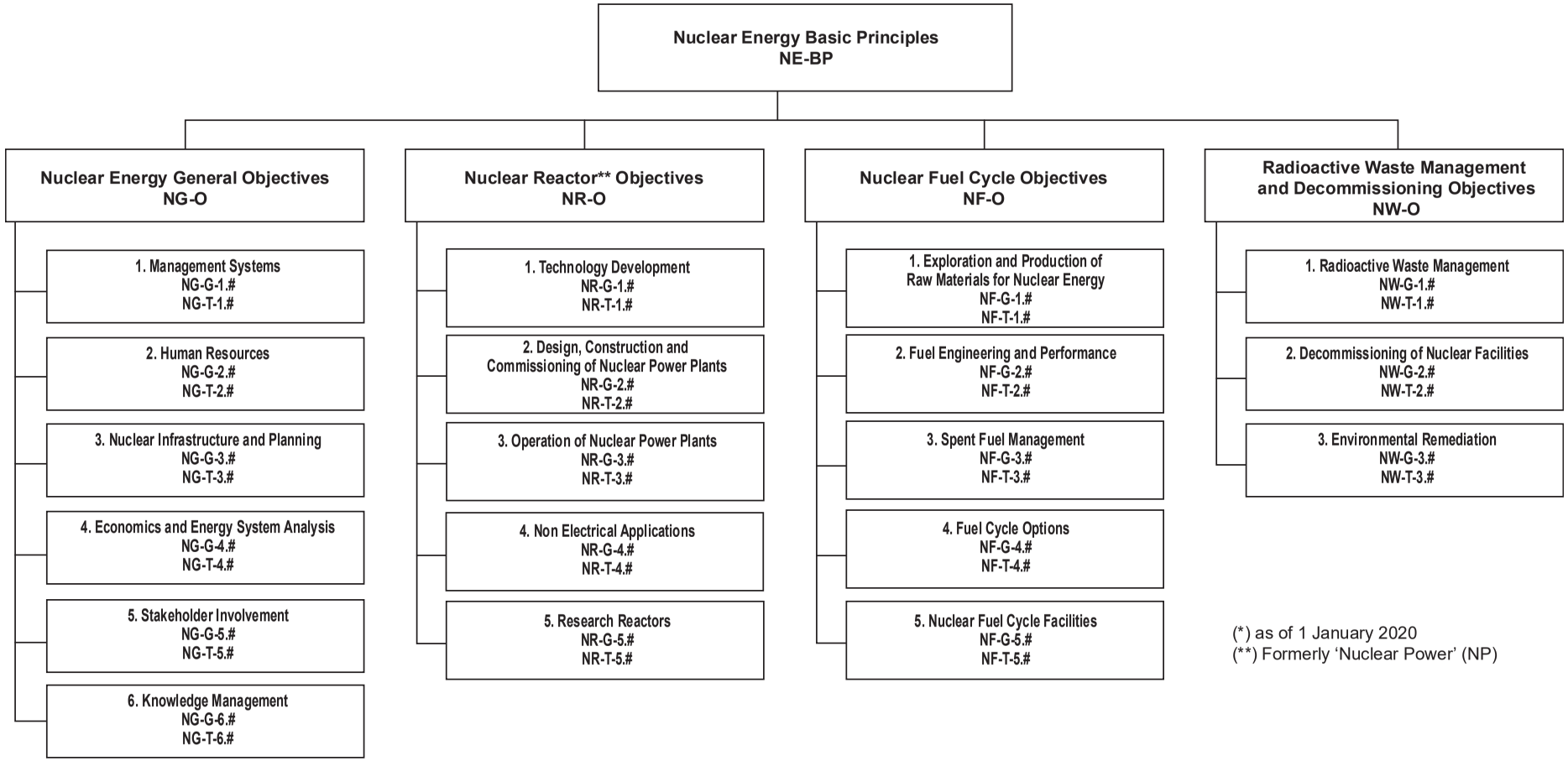
Technical Meeting

Madrid, Spain: 4–7 September 2018

Consultants Meetings

Vienna, Austria: 5–9 February 2018, 4–8 June 2018, 4–8 March 2019

Structure of the IAEA Nuclear Energy Series*



(*) as of 1 January 2020
(**) Formerly 'Nuclear Power' (NP)

Key

BP:	Basic Principles
O:	Objectives
G:	Guides and Methodologies
T:	Technical Reports
Nos 1–6:	Topic designations
#:	Guide or Report number

Examples

NG-G-3.1:	Nuclear Energy General (**NG**), Guides and Methodologies (**G**), Nuclear Infrastructure and Planning (topic **3**), **#1**
NR-T-5.4:	Nuclear Reactors (**NR**)*, Technical Report (**T**), Research Reactors (topic **5**), **#4**
NF-T-3.6:	Nuclear Fuel (**NF**), Technical Report (**T**), Spent Fuel Management (topic **3**), **#6**
NW-G-1.1:	Radioactive Waste Management and Decommissioning (**NW**), Guides and Methodologies (**G**), Radioactive Waste Management (topic **1**) **#1**

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

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

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

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

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

Eurospan Group

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

Trade orders and enquiries:

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

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

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

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

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

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA