|  |
| --- |
|  |
| ONR Technical Assessment Guide  Human Machine Interface (HMI) |



ONR Technical Assessment Guide (TAG)

Human Machine Interface (HMI)

**Head of Profession**: Human and Organisational Capability (HOC)

**Authored by**: Nuclear Inspector

**Approved by**: Human Factors Lead (on behalf of the Head of Profession)

**Issue**: 6

**Published**: May 2025

**Next scheduled review**: May 2028

**Document reference**: NS-TAST-GD-059

**Record reference**: [ONRHH-822789359-20450](https://prodonrgov.sharepoint.com/sites/HOW2Hub/_layouts/15/DocIdRedir.aspx?ID=ONRHH-822789359-20450)

Revision commentary

|  |  |
| --- | --- |
| Issue | Description of update(s) |
| 5.2 | Minor update to references and content transferred across to the latest ONR template. |
| 5.3 | Minor update to extend review date to allow for major review to take place. |
| 6 | Major update which adds clarification and updated references, plus:   * Inclusion of Sections 5.4 and Appendix A discussing HFI * Discussion of SDCV displays in Section 5.8) * Expansion of discussion of Automated and Autonomous Assistive Systems (previously Section 5.8) – now Appendix B |

Contents

[1. Introduction 4](#_Toc198122577)

[2. Purpose and scope 5](#_Toc198122578)

[3. Relationship to licence and other relevant legislation 6](#_Toc198122579)

[4. Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides 7](#_Toc198122580)

[5. Advice to inspectors 12](#_Toc198122581)

[References 28](#_Toc198122582)

[Glossary 30](#_Toc198122583)

[Appendix A – HMI in the HFI lifecycle example activities 31](#_Toc198122584)

[Appendix B – Automated and autonomous assistive systems 32](#_Toc198122585)

# Introduction

1. ONR has established its [Safety Assessment Principles](http://www.onr.org.uk/saps/saps2014.pdf) (SAPs) [1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other dutyholders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR’s inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide (TAG) is one of these guides.

# Purpose and scope

1. This TAG provides guidance to aid inspectors in the interpretation and application of those SAPs related to the Human Machine Interfaces (HMI).   
   It also assists with the application of other SAPs, which set out expectations of a dutyholder’s HMI design and application.
2. This TAG has been written to support assessment activities associated with ONR’s nuclear safety statutory purpose. The guidance presented may also be relevant in relation to ONR’s other statutory purposes namely: nuclear site health and safety; nuclear safeguards; and safety of transport of nuclear and radioactive materials. Nuclear security has a bespoke suite of TAGs which should be used when undertaking assessment activities for that purpose (refer to CNS-TAST-GD-3.3 [2]).
3. This TAG is not intended to be a detailed design guide, nor does it prescribe specific methods and approaches for conducting an assessment of HMI.   
   It provides broad expectations on key points that an experienced human factors (HF) inspector may wish to consider in relation the assessment of HMIs.
4. The aim of the TAG is to advise and inform ONR inspectors in the exercise of their professional regulatory judgement concerning the demonstration of the as low as reasonably practical (ALARP) principle with respect to HMIs. As with all guidance, inspectors should use their knowledge and experience in the depth and scope to which they apply the guidance provided.

# Relationship to licence and other relevant legislation

1. The Nuclear Site Licence Conditions (LCs) place legal requirements on the licensee to make and implement arrangements to ensure that safety is being managed adequately. The LCs provide a legal framework, which can be drawn on in assessment.
2. LCs 14 and 15 (preparation and review of safety cases) apply particularly, and also of relevance are LCs 11 (emergency arrangements), 23 (limits and conditions in the interests of safety), 24 (operating instructions), 27 (safety mechanisms, devices and circuits). Other LCs that touch on the topic of HMI, relate to the design, commissioning and maintenance phases of HMI (for example, LCs 19 – 22 and 28).
3. Regulation 3(1) of The Management of Health and Safety Work Regulations 1999 places a legal requirement on duty holders to produce suitable and sufficient risk assessments and Schedule 1 (d) places the requirement to adapt the work to the individual. In order to be considered suitable and sufficient, such assessments may need to identify and consider the influence of, and need for, suitable HMI as part of the dutyholder’s measures for controlling risk.

# Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides

## SAPs and TAGs

1. ONR’s expectations concerning the suitability of HMI are set out in a number of SAPs. References to HMI, either implicit or explicit, are noted throughout the SAPs and specifically addressed in the sections covering Key Engineering Principles (EKP. 3 to EKP 5), Safety Systems (ESS 3 and 13), Control and Instrumentation of safety-related systems (ESR 1 – ESR 4, 5, ESR 7 & 8), Human Factors (EHF 1–12) and Containment and Ventilation (ECV. 6 and 7).
2. The primary references relating to HMI are contained in the following SAPs:

ESS.3 Monitoring of plant safety:

* Adequate provisions should be made to enable the monitoring of the facility state in relation to safety and to enable the taking of any necessary safety actions during normal operational, fault, accident and severe accident conditions.

Para 400 expands upon ESS 3:

* 400. Monitoring provisions should be classified as safety or safety related as appropriate and should be made: a) in a central control location; and b) at emergency locations (preferably a single point) that will remain habitable during foreseeable emergencies.

ESR.1 Provision in control rooms and other locations:

* Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations.

In addition to referring out to EHF.7, paragraph 430 expands upon ESR 1:

* 430. The systems should provide for control, monitoring and data recording in normal operations, fault conditions and severe accidents. The extent of these provisions should be consistent with the fault analysis and justified in the safety case. See also paragraph 778.

ESR.7 Communications systems:

* Adequate communications systems should be provided to enable information and instructions to be transmitted between locations on and, where necessary, off the site. The systems should provide robust means of communication during normal operations, fault conditions and severe accidents.

ESR.8 Monitoring of radioactive material:

* Instrumentation should be provided to detect the leak or escape of radioactive material from its designated location and then to monitor its location and quantity.

EHF.7 User interfaces:

* Suitable and sufficient user interfaces should be provided at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions.

Para 453 to 456 expand upon EHF.7:

* 453. Appropriate locations include central control rooms, local plant control stations, locations where maintenance and/or testing is carried out and locations identified for monitoring or control within the facility’s emergency preparedness and response arrangements (for example, site emergency control centres (refer to paragraph 783).
* 454. User interfaces, which may be analogue or digital, include controls, indications, alarms, recording instruments, overview displays, mimics, communication equipment, computer-based procedures, computerised operator support systems, intelligent decision aids and reconfigurable displays and controls.
* 455. Plant equipment such as valves, emergency supply connection points and similar plant and equipment are also considered to be user interfaces.
* 456. User interfaces should be designed to ensure compatibility with the psychological and physical characteristics of the intended users and to facilitate reliable human performance. Interfaces and equipment should be clearly labelled.

The user interface should:

1. provide sufficient, unambiguous information for the operator to maintain situational awareness in all operating modes and in fault and accident conditions (for example, the behaviour and status of the automated plant control systems);
2. provide a conspicuous early warning of any changes in parameters affecting safety;
3. provide a means of signalling safety system challenges and of confirming that the safety system has initiated and achieved its safety functions;
4. support effective diagnosis of plant deviations; and
5. enable the operator to determine and execute appropriate actions including those needed to overcome failures of automated safety systems or to reset a safety system after its operation; and
6. support communication between personnel located in the same or different operating locations, including locations external to the facility or site.
7. Closely linked to EHF.7 are SAPs EHF.1 Integration with design, assessment and management (refer to NS-TAST-GD-058 [3]) and EHF 2 Allocation of safety actions (refer to NS-TAST-GD-064 [4]), which are essential supporting activities in the design of a safe and operable HMI.
8. In addition, SAPs EHF.5 Task analysis and EHF.10 Human reliability (refer to NS-TAST-GD-063 [5]), EHF. 6 Workplace design (refer to NS-TAST-GD-062 [6]), ESS.9 Time for human intervention (refer to NS-TAST-GD-010 [7]) and ESS.13 Confirmation to operating personnel are also relevant.
9. A number of ONR TAGs provide guidance to inspectors on aspects that form part of the HMI TAG, or interface directly with it. Where relevant, these TAGs are referred directly in Section 5 and linked to the relevant SAPs above.

## IAEA Safety Standards

1. The guidance is also broadly consistent with IAEA standards and guidance. Key relevant IAEA publications are referenced in section 5 of this TAG.
2. The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2014 and are recognised by ONR as relevant good practice. They should therefore be consulted, where relevant, by the inspector.
3. Key relevant IAEA publications are:

* SSG-51 – Human Factors Engineering in the Design of Nuclear Power Plants [8]
* SSR-2/1 – Safety of Nuclear Power Plants: Design [9]
* SSG-39 – Design of Instrumentation and Control Systems for Nuclear Power Plants [10]
* NR-T-2.12 – Human Factors Engineering Aspects of Instrumentation and Control System Design [11]

## WENRA Reactor Safety Reference Levels

1. The guidance in this TAG is consistent with WENRA Safety Reference Levels (SRLs) [12]:

* Issue E (Design Basis Envelope for Existing Reactors): E10. Instrumentation and control systems
* Issue F (Design Extension of Existing Reactors): F4. Ensuring safety functions in design extension conditions
* Issue LM (Emergency Operating Procedures and Severe Accident Management Guidelines): LM4. Verification and validation
* Issue O (Probabilistic Safety Analysis (PSA)): O1. Scope and content of PSA

1. The guidance in is also consistent with SRLs Waste and Spent Fuel Storage [13], Decommissioning [14], Radioactive Waste Disposal Facilities [15] and Existing Research Reactors [16].

## Other

1. The advice contained herein is also reflected to a greater extent in a number of other standards and guidance related to the effective design of HMI. Examples of comprehensive standards that ONR recognises as sources of relevant good practice are provided are:

* US Nuclear Regulatory Commissions, NUREG 0700 - Human – System Interface Design Review Guidelines [17]
* Ministry of Defence, Human Factors Technical Guides, Section 3 Equipment [18]
* Engineering Equipment and Materials Users Association, EEMUA Publication 191 - Alarm systems - a guide to design, management and procurement [19]

1. The following British and ISO standards may also be applicable to the topic of HMI:

* BS EN IEC 60964:2019 Nuclear power plants. Control rooms. Design
* BS EN 60965: 2016 Nuclear power plants. Control rooms. Supplementary control room for reactor shutdown without access to the main control room
* BS IEC 62954:2021 Nuclear power plants. Control rooms. Requirements for emergency response facilities
* BS EN 61227:2016 Nuclear power plants. Control rooms. Operator controls
* BS EN 62241:2015 Nuclear power plants. Main control room. Alarm functions and presentation
* BS EN IEC 62682:2022 Management of alarm systems for the process industries
* BS IEC 61772:2013 Nuclear power plants. Control rooms. Application of visual display units (VDUs)
* BS EN IEC 62646:2019 Nuclear power plants. Control rooms. Computer-based procedures
* BS EN ISO 11064- (All Parts): Ergonomic design of control centres
* BS EN ISO 9241- (All Parts): Ergonomics of human-system interaction.
* BS EN 61839:2014 Nuclear power plants. Design of control rooms. Functional analysis and assignment
* BS EN 61508-2:2010 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems.
* BS IEC 63351:2024 Nuclear facilities — Human factors engineering — Application to the design of human-machine interfaces
* BS EN IEC 63303:2024 Human machine interfaces for process automation systems

**Note:** Specific references to the available standards and guidance on HMI are not made in the text as they would be too numerous.

# Advice to inspectors

## Definition of Human Machine Interface

1. Humans play a key role in the safe and efficient operation of nuclear facilities. Plant and facility HMIs which enable the operator to control the plant and manage nuclear safety are important in supporting this role. Operators contribute to a plant’s defence-in-depth hierarchy in a number of ways including the prevention and control of abnormal operation, detection of failure, control of faults within the design basis and accident/emergency response. Therefore, nuclear facilities and their safety cases may identify human errors, human actions and administrative controls in respect of reliable interventions for monitoring and control of both normal and abnormal conditions.
2. HMIs are the principal mechanism through which personnel understand, interact with and control the plant and processes. They provide the facilities for information transfer and interaction in the form of various instrumentation, displays, alarms and controls. HMIs supports the delivery of nuclear plant safety functions related to detection, diagnosis, decision-making and action. In nuclear facilities, information is typically displayed, and the plant controlled using conventional physical (traditionally analogue) or virtual / screen-based (digital) technology or a combination of these types. Operator interactions can range from controlling or supervising normal operations to manually intervening in nuclear processes in the event of automation failures to establish a safe and stable state. HMIs need to support all operational states including normal, abnormal and fault conditions.
3. There are no strict definitions for these different types of HMI. Instead, it is more appropriate to consider them based on their characteristics. HMIs range from conventional physical controls and displays through to systems where the (virtual) operational controls are accessed on some form of screen through to advanced HMIs which may incorporate some level of automation.
4. Conventional physical (analogue) HMIs typically feature one-to-one mapping of the control to the function or the instrumentation to the sensor (or have a small number of sensor channels with the ability to switch between). For example, a hand-wheel used to open and control a valve, or a push button that closes a control circuit thus remotely opening a valve.
5. HMIs where control is enacted via a screen can include those where a button (physical or virtual) transmits a different signal / initiates a different sequence via a programmable system dependent on context (on-screen labels associated with controls change as task progresses).
6. Advanced HMIs (which are commonly digital) comprise multiple functions and instruments, which are mapped onto (typically) a number of visual display units (VDUs). Another feature these screen-based HMIs is their ability to support high levels of automation and operator assistance systems. Further guidance on assistive systems is provided in Appendix B of this TAG.
7. ONR recognises that HMIs can take a wide range of formats and regulate their use in a technology neutral way.
8. The level of automation / computerised support in the delivery of a function or functions and the corresponding requirements for reliability or integrity is a separate issue which should receive specific consideration jointly by Control and Instrumentation (C&I) and HF inspectors.
9. When interacting with HMI, personnel are often required to complete two activities.

* The primary task of using the information presented on the HMI and initiating any appropriate control actions.
* Secondary tasks that interface access and manage tasks required to complete the primary task. For conventional physical HMI, this might involve moving around the plant to various control/display locations. For computer-based systems, this might involve navigating between different screens on the same system or amalgamating information from across different, diverse data sources.

1. Therefore, the design of any HMI needs to be compatible with the level of performance required of the operator and be based on the type of operator tasks it is required to support.
2. HMI are commonly located in purpose-built control rooms but there are also interfaces distributed through a facility to permit local-to-plant monitoring and/or control in other locations throughout the site (e.g. support facilities and offices). Most HMI are supported by C&I or mechanical systems. However, there are other examples, like passive indications used to measure levels (e.g. depth gauge boards using to measure water levels, loose nut indicators on vehicles, physical position indicators on cranes, etc.), which may be independent of such systems. It therefore follows that relevant good practice in ergonomics should be included and evident in all the licensee’s design and modification activities.

## 

## General regulatory approach

1. This TAG provides guiding principles to inform inspectors’ expectations regarding how a dutyholder will demonstrate that HMI provisions will support effective human performance and are suitable and sufficient. In particular, those expectations regarding the dutyholder’s demonstration of the feasibility of delivering human actions and administrative controls and reducing risks so far as is reasonably practicable (SFAIRP). The guidance provided in this section is applicable to the assessment of all types of HMI.
2. Where safety important human actions are required, and their need is justified by the dutyholder, the feasibility and reliability of those actions should be demonstrated to be effectively supported by suitable and sufficient HMI. Inspectors should have confidence that the dutyholder’s process adequately identifies requirements for the HMI to support human actions and administrative controls, and the demonstration of their ergonomic adequacy in-line with relevant good practice (RGP).
3. All HMIs, not just those directly incorporated into safety systems, should be designed appropriately and comply with RGP. Non-safety-related HMIs have the potential to impact human actions and administrative controls, either by being co-located to safety-related HMI or by communicating similar information. A guiding principle is that co-located HMI should share common display and control characteristics where reasonably practicable to do so. Consistency of HMI throughout the plant should also be maintained where it is reasonably practicable to do so.
4. The key elements for ensuring the provision of suitable and sufficient HMI to support safe management and operation of nuclear plant are the understanding of:

* The plant context as built (with appropriate consideration given to the potential changes through life),
* The nature of the human actions and administrative controls related to the delivery of plant safety functions and operating rules,
* Key operational requirements and targets, and
* End user characteristics.

1. Understanding of these aspects should be incorporated into an effective and integrated through-life process for the design, operation and maintenance of HMIs.
2. Inspectors may consider whether:
3. The need for, and level of reliance on, HMI (and operator actions) to perform important safety functions have been justified on ALARP grounds.
4. The dutyholder’s incorporation of HMI within a design is demonstrated in an overall design philosophy and approach (NS-TAST-GD-058 [3] uses the term ‘Concept of Operations’ to describe this). The main safety and operability targets for the HMI system should be specified.
5. The dutyholder has used its safety case to specify requirements for the HMI and has completed a proportionate level of task analysis to inform its design and/or modification.
6. The dutyholder has proportionally integrated HF / ergonomics RGP into all areas of HMI design. This should not focus solely on the more high-profile HMIs such as the main control room.
7. The HMI design is included as part of the dutyholder’s Human Factors Integration (HFI) process which should have clear links to the dutyholder’s project, design, engineering and procurement processes.
8. The dutyholder has declared and justified the standards used for the design / modification and substantiation of its HMI. A HMI style guide, or similar document, based on agreed HMI requirements and specifications should be developed by the dutyholder to demonstrate the philosophy and underlying principles for the HMI and the integration of these requirements and specifications into the design. The style guide defines the design and interaction principles in the HMI design. Note that where non-UK standards are proposed / used, the dutyholder should consider any differences in conventions which are contrary to UK good practice standards.
9. Where dutyholders develop and adopt in-house standards on the design and layout of the HMI, the dutyholder should clearly set out the standards and guidance proposed / used. These should be justified to the extent that they demonstrate compliance with RGP.
10. The dutyholder has specified safety and operability criteria and provided evidence in its safety case and design documentation that the HMI design and substantiation meets these and will continue to do so throughout its lifetime.
11. The dutyholder has considered and taken into account the capabilities, characteristics and numbers of the HMI user population, during specification and design. RGP is for such information to be presented in a Target Audience Description (TAD) document. This minimises the risk of unsubstantiated assumptions about end users of the HMI being made throughout the design process.
12. The dutyholder’s process for identification of HMI requirements covers all plant operational modes / states including normal operations, maintenance, testing and calibration activities, fault and emergency response.
13. There is a clear documented process that demonstrates how the dutyholder has managed and resolved any conflicts and trade-offs associated with HMI, for example, between safety constraints and ergonomics best practice.
14. The dutyholder has carried out an operational experience review (on existing or similar plants), including, where reasonably practicable to do so, a review of any simulations or mock-ups of its proposed HMI applications or modification, particularly in plants with a similar concept of operations. The fidelity of these simulations / mock-ups should be appropriate for the lifecycle stage and the reviews being undertaken (simple paper-based mock-ups can be very effective).
15. Allocation-of-function analysis has been used to inform and support the design (and modification) of HMI.
16. The design and operational concept of HMI has been used as input to the development of procedures and operator training needs / competence requirements.
17. The dutyholder has conducted suitable HF / ergonomics evaluation and testing / trials of the design, development and use of HMI and that this has demonstrated that the HMI is effective in supporting personnel in all operational states. Where testing has identified HF deficiencies in the design, evidence is available that they have been addressed and that, where appropriate, the design has been re-tested and demonstrated as safe and operable. It is expected such evaluation is undertaken throughout the system lifecycle, for example as part of periodic safety review [20].
18. The HMIs available to operators supports the demonstration of on-going compliance with operating rules [21], that parameters remain within the safe operating envelope, and the dutyholder has considered matters such as redundancy and diversity for circumstances where HMIs may fail or become unavailable.
19. The dutyholder has used its design and / or review of HMI to inform the assumptions and claims made in its Human Reliability Assessment (HRA) and associated qualitative and quantitative safety assessments, so confirming that that those assessments remain valid throughout the operation of the system.
20. The dutyholder has provided evidence that the reliability of the HMI is sufficient for the risk importance of the related human actions and administrative controls. It should be recognised that diversity and redunancy of HMI and supporting systems may be required to achieve the reliability required to support the claimed actions impacting safety. Consultation with other ONR discipline Inspectors may be required to confirm an appropriate HMI equipment classification.

## HMI design considerations

1. This section provides general advice to the inspector regarding good practice expectations for HMI design. The principal aim of the HMI should be to support reliable task performance, in particular, of human actions and administrative controls identified in the safety case.
2. It is important that any HMI is compatible with end user capabilities, population norms / stereotypes and demonstrably supports the operator in the operational control and monitoring of the facility. This applies to all anticipated operational states.
3. The design of HMI should (summary of list provided in IAEA SSG-51 [8]):

* Accommodate the different roles and responsibilities of the various users expected to interact with the system.
* Be designed with primary attention given to the role of the operator who is responsible for the safe operation of the equipment.
* Provide an effective overview of the plant status.
* As far as is reasonable practicable, apply the simplest design consistent with function and task requirement.
* Present information such that it can be rapidly recognised and understood by operators (taking into account HF RGP).
* Accommodate failure of physical and screen-based HMI equipment without significant interruption of control actions.
* Reflect consideration of human cognition, physiological characteristics, characteristics of human motor control and relevant anthropometry.

1. Inspectors may consider whether:
2. The dutyholder selection of HMI equipment, takes into account task demands, the working environment in which it shall be used and broader ergonomics RGP. For example, touch screens technologies enable highly flexible HMIs but covnetional keys / buttons are more suited to alphanumeric data entry, fine motor control and environments prone to movement / vibration. Additional considerations for the selection of local to plant and mobile HMI equipment include charateristics such as robustness, weatherproofing, portability and battery life.
3. The dutyholder has ensured that the design of the HMI provides sufficient and unambiguous information to the operator to maintain situational awareness[[1]](#footnote-2) in all plant states [4]. The dutyholder has applied appropriate and consistent coding, labelling, grouping, navigation and layout principles for the design of all relevant HMI controls and displays that are suitable for the tasks to be performed and all personnel who may use the HMI.
4. The dutyholder’s HMI ensures that the presentation of information and controls are appropriate for their purpose, support required response times and minimise the potential for errors. Where tasks are completed in different locations (e.g. control room and local to plant) or in the same location with different HMIs (e.g. physical and screen-based HMIs within the same control room), consistent HMIs should be provided. Any task analysis / substantiation should give due consideration to the totality of HMIs available to support task performance.
5. The dutyholder has assessed the cognitive and physical workload and task demands associated with the HMI design, and its use in all foreseeable plant states including the most onerous states and fault conditions. The HMI provides for the fluent execution of those tasks which include cognitive elements, minimising demands for high memory load and complexity.
6. The HMI equipment and workstations are arranged within the workplace in a safe and accessible location, and in a way that is consistent with users’ task requirements and expectation for all foreseeable plant states. Where appropriate, link analysis has been used to inform decisions regarding the distrubution and placement of HMIs with the workspace.
7. The dutyholder’s HMI offers the user adequate plant and process status feedback and, where safety critical information is presented, failure modes associated with the HMI (for example, loss of or corrupted data) are revealed and not likely to exacerbate fault conditions by misleading operators or making responses difficult.
8. The dutyholder is able to demonstrate that suitable and sufficient alternative or back-up HMI are available to cope with HMI failures or other scenarios when primary HMIs may not be available. Redundant and diverse HMI should, where reasonably practical, be consistent with the primary HMI design philosophy.

It should be confirmed that the dutyholder has specifically considered how the back-up HMI will be operated and demonstrated that migrating control is achievable and reliable. For example:

* 1. Where elements of the primary HMI have failed, including where the user has to work from back-up HMI.
  2. In degraded work environments or when Personal Protective Equipment (PPE) must be worn.
  3. How authority is passed from control station to control station or operator to operator.

1. The dutyholder has considered the impact of inadvertent activation of controls and has designed the HMI to minimise the likelihood of, and be tolerant to, these types of error.
2. The dutyholder has considered maintenance requirements of the HMI and has designed it such that the likelihood of maintenance errors is reduced and safety consequences minimised.
3. The dutyholder’s choice of the type, amount and style of information presentation via the HMI is justified as most appropriate to support the tasks required. This should inform / interact with the selection of physical HMI equipment (e.g. screen size, resolution, colour reproduction, etc.).
4. The physical design, layout and operation of HMI are demonstrated to be compatible with task requirements, user characteristics and the expectations of the operator to adequately and safely support human performance, and specifically human actions and administrative controls.
5. Required control actions and corresponding feedback/response communicated via HMI is consistent across the site/facility and compatible with operator expectations.
6. Where possible, end user representatives have been involved throughout the entire design lifecycle of the HMI.

## Human Factors Integration (HFI)

1. In order for HMI to be appropriately designed / meet the needs of the users and support the safety function delivery, the HMI design needs to be appropriately integrated into the wider safety assessment and engineering design / procurement activities. NS-TAST-GD-058 [3] details regulatory expectations relating to the design and safety case aspects of HFI, and should be read in-conjunction with this HMI TAG.
2. It can be useful to consider HMI-related HFI activities within a “V model”, a model typically used as a graphical representation of the systems development lifecycle. An example is presented in **Figure 1**. Such models are particularly useful in demonstrating the expected lifecycle for HF requirements – they should be identified early, refined as the design develops and verified and validated through prototyping, testing, commissioning and operation.
3. The appropriate timing of relevant HFI tasks is of utmost importance to ensure HF analysis appropriately informs, and is integrated within, broader project activities. Inspectors should ensure that HF work aligns / is maturing at the same pace as engineering and safety analysis activities, ensuring options are not foreclosed and the resulting human tasks can be reliably performed. For example, design features and system integration options (HMI and alarm options) can be limited by the (limited) functionality of the selected hard or software solution. It is therefore important that key HF requirements are identified early in the lifecycle (e.g. definition and concept design) so they receive due consideration at relevant decision points.
4. Appendix A of this TAG presents a summary table outlining design phases and associated phased safety case submissions and related HF and HMI considerations. This table is intended to guide Inspectors by illustrating a potential progressive approach to HFI for HMI. It is not intended to be a prescriptive or fully comprehensive list of regulatory expectations.

A diagram of a design process

AI-generated content may be incorrect.

Figure 1 - Role of safety function categorisation (green box) and SSC classification (blue box) within the lifecycle model (‘V-diagram’)

1. Further guidance on the topic of HFI for HMIs can be found in:

* IAEA, Human Factors Engineering Aspects of Instrumentation and Control System Design, IAEA Nuclear Energy Series No. NR-T-2.12 [11]
* ISO 9241-110:2020, Ergonomics of human-system interaction. Part 110: Interaction principles
* ISO 11064-1:2000 Ergonomic design of control centres. Part 1: Principles for the design of control centres
* BS IEC 63351:2024 Nuclear facilities — Human factors engineering — Application to the design of human-machine interfaces

## Overview screens and mimic displays

1. Improvements in screen display technologies have provided opportunity for larger and higher resolution displays that allow increasing amounts of information / data to be presented within an HMI. Such technologies have been exploited within modern control room environments to present overview displays. Increasingly, large format screen-based HMI are being used instead of more conventional panel-based interfaces to display process information. Desktop screen-based systems, which display information to single users, may also be used.
2. The main objective of an overview display is to provide an array of key information that can be scanned by the operational team to gain a rapid appraisal of a plant or process state. Overview screens are designed to enhance situational awareness of critical plant parameters and conditions. Large displays that can be shared by multiple personnel to facilitate the development of a common understanding of plant conditions.
3. It is important that overview displays are designed to support the level of decision-making that they will be used for, as during off-normal, accident or emergency situations they can become the focal point of the team.
4. Inspectors may consider whether:
5. The dutyholder has provided a justification of how overview screen(s) will be used, which should include a discussion on whether the design will be tailored to either strategic or tactical decision making. In addition, the expectation should be that the overview screen(s) meets HF / ergonomics RGP and are compatible with other HMI in the plant.
6. Where they exist, or are proposed, large overview display(s) may allow operators to monitor the results of each other’s activities in order to detect and correct errors or to lend prompt support where required.
7. Mimics[[2]](#footnote-3) are also used as operator support tools, which encourage operators to form accurate mental models of system functions. They are designed to ensure that the operator can accurately understand the processes and functions to which the mimic relates. Care is needed in their design as the manner in which mimics are laid out is often the basis of the user’s understanding of the system and can significantly impact how they diagnose problems and make subsequent decisions. It may be appropriate to have different mimics that highlight the differing relationships between components under different plant conditions (for example, different mimics for normal operations, shutdown, specific fault /emergency conditions, etc.).
8. Inspectors may consider whether the duty holder has provided a rationale for the style (for example, task versus plant-based displays) and the degree of detail on any mimics including the specification of conventions to be applied.
9. Further guidance on this topic of mimic and overview displays can be found in:

* BS EN IEC 63303:2024 Human machine interfaces for process automation systems
* Engineering Equipment and Materials Users Association, EEMUA Publication 201 – Control Rooms: A guide to their specification, design, commissioning and operation [22]

## Emergency shutdown / post accident monitoring HMIs

1. The main purpose of emergency shutdown (ESD) HMI is to enable the operator to take the plant to a safe, stable, and then shutdown, state, where the conditions of the accident permit. Where the conditions do not permit, the post accident monitoring (PAM) HMI should provide the capability to monitor parameters that are needed for incident management purposes. These may include temperature, reactivity, pressure, containment and safety system activation status.
2. Inspectors may consider whether:
3. ESD / PAM HMI are consistent with relevant good practice and with other HMI across the site/facility. They should also be designed with due consideration of the likely work environment that may be encountered under such conditions (for example, fire, flood, seismic activity, etc.).
4. The dutyholder has provided evidence that demonstrates that the HMI at emergency locations provides all the necessary plant status information and control functionality needed by to deliver the required emergency response actions.
5. Where reasonably practicable, the use of the HMI has been tested / exercised in a high-fidelity simulation to demonstrate its effectiveness (for example, wearing of anticipated PPE / RPE), limited illumination, smoke, etc.). Careful consideration should be given to the level of fidelity required of tests and exercises.

## Communication system considerations

1. Although communication system design is too complex to cover in detail within the scope of this TAG, there are a number of important issues for the inspector to consider that relate to human actions and administrative controls underpinned by reliable communication:
2. Where communications equipment is key to achieving a safe stable state, it needs to remain available under the anticipated fault conditions.
3. Whether there are alternative communication channels available (i.e., verbal and non-verbal) and where they are located relative to the task(s) being performed.
4. The information needing to be transmitted.
5. To whom it needs transmitting.
6. When it needs to be transmitted (for example, is information needed immediately).
7. The clarity with which the information needs transmitting.
8. What the receiver will be expected to do with the information.
9. The dutyholder should have considered all of the foreseeable operating conditions that the communications system will have to function under, for example, during and following a fire, flood, seismic event, during extreme weather conditions, under high environmental noise levels. The effect of PPE / RPE and psychological factors such as stress should also be considered.
10. Inspectors may consider whether:
11. The design of the dutyholder’s communications system is matched to the requirements and most onerous foreseeable conditions under which it is expected to operate. This is based on the safety case and command and control needs.
12. The dutyholder has provided evidence that the design of the communications system will function under all required conditions, especially if the safety case claims that personnel will use the communication system as part of their normal, abnormal, accident and emergency activities. Where possible this should be tested/exercised under realistic conditions.
13. Particular attention has been given to whether the system will be effective in areas of very high noise or will remain functional under internal and external hazard conditions.
14. The dutyholder has produced a communications plan detailing how the system/s will be used.

## Control room / centre design considerations

1. It is beyond the scope of this TAG to go into detail on the non-HMI elements of control room / control centre design. The inspector is referred to [6] and other sources of relevant good practice listed therein. Control rooms are now often part of larger control centres, which may include a central control room and secondary control rooms with associated support facilities such as offices, welfare facilities, etc.
2. Inspectors may consider whether:
3. The dutyholder has considered the effects of any additional functions and secondary users in the design, testing and validation / verification of the control centre design. It is not acceptable to test just the HMI in isolation.
4. The dutyholder has considered the full needs of the primary user in terms of all the activities that are carried out within the control room. For example.
   1. Is adequate space provided for the plant and instrumentation drawings, or hard-copy procedures to be viewed?
   2. Have areas been provided where strategic incident management discussions can be held so as not to distract the operators managing the tactical elements of the incident?
5. Where the dutyholder proposes to have multiple control rooms (for example, emergency control rooms, work execution control centres, plant outage control rooms, etc.), the same standards and principles have been applied to their design and operation. In addition, these areas and the HMI they house, are consistent with ergonomic RGP and conventions used elsewhere in the site / facility HMI.
6. The dutyholder has considered all appropriate environmental HF issues for all foreseeable plant states. Post event habitability is a key area of interest.
7. In most extant control rooms on UK nuclear sites, operators have permanent access to the status of the most safety significant indications and alarms via conventional panels with physical illuminated annunciators. Such displays are referred to as Spatial Dedicated Continuously Visible (SDCV) displays. SDCVs are extremely useful since the operator can quickly scan the panel and diagnose the plant condition via the pattern of dark and illuminated annunciators. It is good practice to replicate SDCV functionality in “digital-only” control rooms (i.e. dedicated screens with minimal requirements for HMI navigation to access safety significant indications).

## Alarm system considerations

1. Alarm system design, and the role it plays in the delivery of nuclear safety functions, is a complex issue which can not be covered in detail within this TAG. This section identifies some key issues inspectors may want to consider when assessing the adequacy of these systems.
2. Alarms and alarm systems often form an integral aspect of an HMI. They may provide or contribute to those safety functions that are claimed to maintain a plant within a safe operating envelope and help operators recognise and respond to a fault.
3. Alarms can be supported by warnings and alerts.

* Warnings advise operators that a parameter is approaching a pre-defined setting or warning of the potential hazards associated with a course of action.
* Alerts advise context important information that does not require any action, for example a change of plant state.
* Warning and alerts should be separated from alarm signals where it is reasonably practical to do so.

1. Requirements for alarms will come from the safety case, industry practice and historical precedence. However, because of the ease of implementing alarms into modern systems, there is a danger that the number included in the HMI design will exceed the cognitive workload capabilities of the operator or their needs for information. It is therefore important that each alarm and warning is carefully selected and categorised, and that the overall process, and each decision, is justified and documented by the dutyholder.
2. Every alarm should have a clearly defined operator response. If a response cannot be defined, then the signal generated by the HMI should not be an alarm (although it may constitute a warning or an alert or take the form of a log entry that does not need a response from the operator during the progression of an incident).
3. Inspectors may consider whether:
4. The dutyholder has an alarm design and management strategy document, which includes an overall philosophy for the design and management of alarm systems.
5. The dutyholder has justified the need for, and properly engineered its alarm systems within its overall HMI.
6. The dutyholder’s alarm system prioritisation, engineering configuration and coding is consistent: across the site/facility, with the safety significance of operator response actions claimed in the safety case, and with the overall alarm philosophy.
7. The dutyholder has presented a soundly based appreciation of alarm configuration during fault handling conditions such that there is confidence that alarm conditions will enhance decision making and reliable initiation of recovery actions.
8. All safety-related alarms, their settings and priorities are presented in a quality-controlled alarm schedule or similar document.
9. The dutyholder can demonstrate that required responses to alarms are supported by suitable alarm response instructions.
10. The dutyholder’s reliability claims on an alarm system include the reliability of the alarm and that of the operator responding to the alarm. Also, whether, such claims should be substantiated; either by reference to a comparable alarm system elsewhere, or by means of alarm handling trials in the case of a novel system. ONR expects dutyholders to take cognisance of the relevant good practice contained within [19] (or equivalent), which limits the amount of risk reduction that can be claimed using alarms.
11. The dutyholder’s alarm system meets with general ergonomic RGP for HMI.
12. The dutyholder has set performance targets for the alarm system, undertakes regular reviews and uses the findings of such reviews to inform decision making. Good examples of these can be found in [19].
13. Further guidance on the topic of alarm systems can be found in:

* Engineering Equipment & Materials Users' Association (EEMUA) 191 – Alarm systems - a guide to design, management and procurement [19]
* BS EN IEC 62682:2022 Management of alarm systems for process industries

## HMI modification / modernisation considerations

1. The IAEA states that there are a number of specific issues that need to be considered during the modernisation of existing HMI [23]:
2. It may be necessary to reconstruct the design basis of the plant.
3. Even with an existing design basis, it may be necessary to interpret its requirements for digital C&I.
4. Compromises may have to be made because the project has to adapt to the existing plant and its operational requirements.
5. The key HF issues associated with modification / modernisation relate to how well new equipment will integrate with what is extant and end user acceptance and how these factors may affect user performance. It may be that existing HMI uses technology, coding or functionality conventions that are no longer consistent with HF / ergonomics RGP. Even in instances where the conventions are compatible, there will be considerable training and procedural overheads associated with such a project.
6. Inspectors may consider whether:
7. The dutyholders HMI modification / modernisation project is being informed by RGP. Significant projects should be carried out in line with the expectations for a new build.
8. Proposals to modify / modernise systems should, where appropriate, be subject to proportionate application of the licensee’s LC22 (Modification or experiement on exisitng plant).
9. The dutyholder has provided a justification for the decision to either design the new equipment to meet the extant HMI conventions (that may not fully align with current HF/ergonomics best practice), or to operate two levels of HMI with different coding and functional conventions with all the associated transfer of training and procedure issues. Such HMI modification / modernisation decisions and their impact should be clearly reflected in the dutyholder’s safety case and HRA and demonstrated to reduce risks to ALARP.
10. The dutyholder has assessed the risks associated with the transition from the extant HMI to the modified / new system and has adequate arrangements in place to ensure that such risks are managed ALARP. Topics of interest include training, procedures, and the impact on/update of simulators. Any periods of proposed parallel running of extant and new systems should receive specific attention.

# References

|  |  |
| --- | --- |
| [1] | ONR, “Safety Assessment Principles (SAPs) for Nuclear Facilities - 2014 Edition (Revision 1),” 2020. |
| [2] | ONR, “CNS-TAST-GD-3.3 Workspaces, equipment and user interfaces”. |
| [3] | ONR, “NS-TAST-GD-058 - Human Factors Integration”. |
| [4] | ONR, “NS-TAST-GD-064 - Allocation of Function between Human and Engineering Systems”. |
| [5] | ONR, “NS-TAST-GD-063 - Human Reliability Analysis”. |
| [6] | ONR, “NS-TAST-GD-062 - Workplaces and Work Environment”. |
| [7] | ONR, “NS-TAST-GD-010 Early Initiation of Safety Systems”. |
| [8] | IAEA, “INTERNATIONAL ATOMIC ENERGY AGENCY, Human Factors Engineering in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-51,” Vienna, 2019. |
| [9] | IAEA, “INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1),” Vienna, 2016. |
| [10] | IAEA, “INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39,” Vienna, 2016. |
| [11] | IAEA, “INTERNATIONAL ATOMIC ENERGY AGENCY, Human Factors Engineering Aspects of Instrumentation and Control System Design, IAEA Nuclear Energy Series No. NR-T-2.12,” Vienna, 2021. |
| [12] | WENRA, “WENRA Safety Reference Levels for Existing Reactors,” 2020. |
| [13] | WENRA, *Waste and Spent Fuel Storage Safety Reference levels. Version 2.2,* 2014. |
| [14] | WENRA, *Decommissioning Safety Reference Levels. Version 2.2,* 2015. |
| [15] | WENRA, *Radioactive Waste Disposal Facilities Safety Reference Levels,* 2014. |
| [16] | WENRA, *Safety Reference elves for Existing Research Reactors,* 2020. |
| [17] | US Nuclear Regulatory Commissions, “NUREG 0700 - Human – System Interface Design Review Guidelines,” 2020. |
| [18] | Ministry of Defence, “Human Factors Integration Management System - Human Factors Integration Technical Guides - Section 3 Equipment”. |
| [19] | Engineering Equipment and Materials Users Association, “EEMUA Publication 191 - Alarm systems - a guide to design, management and procurement - 4th Edition, November 2024”. |
| [20] | ONR, “NS-TAST-GD-050 - Periodic Safety Reviews (PSRs)”. |
| [21] | ONR, “NS-TAST-GD-035 - Limits and Conditions for Nuclear Safety (Operating Rules)”. |
| [22] | Engineering Equipment and Materials Users Association (EEMUA), “Publication 201 – Control Rooms: A guide to their specification, design, commissioning and operation,” Edition 2, 2019. |
| [23] | IAEA, “NP-T-1.4 - Implementing Digital Instrumentation and Control Systems in the Modernisation of Nuclear Power Plants,” 2009. |

# 

# Glossary

AI Artificial Intelligence

ALARP As low as reasonably practicable

AoF Allocation of Function

BS British Standard

C&I Control and Instrumentation

EEMUA Engineering and Equipment Materials Users’ Association

EFHA Early Human Factors Assessment

ESD Emergency Shutdown

HF Human Factors

HFI Human Factors Integration

HMI Human Machine Interface

HOC Human and Organisation Capability

HRA Human Reliability Analysis

IAEA International Atomic Energy Agency

ISO International Standards Organisation

ISV Integrated System Validation

LC Licence Condition

ONR Office for Nuclear Regulation

OPEX Operating Experience

PAM Post Accident Monitoring

PCmSR Pre Commissioning Safety Report

PCSR Pre Construction Safety Report

PPE Personal Protective Equipment

PRS Periodic Review of Safety

PSA Probabilistic Safety Analysis

PSR Preliminary Safety Report

RPE Respiratory Protective Equipment

SAP Safety Assessment Principle

SDCV Spatial Dedicated Continuous Display

SFAIRP So far as is reasonably practicable

SRLs Safety Reference Levels

TAD Target Audience Description

TAG Technical Assessment Guide

UK United Kingdom

US NRC United States Nuclear Regulatory Commission

VDU Visual Display Unit

VR Virtual Reality

WENRA Western European Nuclear Regulators’ Association

# Appendix A – HMI in the HFI lifecycle example activities

| System maturity phase | Problem definition / concept stage | Detailed design / design freeze | Implementaiton / construction | Test and commissioning | Operations |
| --- | --- | --- | --- | --- | --- |
| *Staged safety submission* | *PSR* | *PCSR* |  | *PCmSR* | *PRS* |
| HF topics | Review of OPEX  EFHA  Early optioneering (initial AoF)  Target auidance desciption  Concept of ops  Functional spectification (Ops)  Alarm philosophy  HMI style guide | Application of HF RGP via reqs.  Workplace design and layout  Environmental conditions defined  Detailed optioneering  AoF justification  Task design  HMI design  Procedure design  Identification and design of admin controls  Staffing concept including shift patterns  Identify training needs | Verification of HR reqs.  Task verification  Further development of procedures  Further development of admin controls  Staffing arrangements  Training development | Validation of HF reqs.  Validation of workspace layout  Validaiton of environmental conditions  Validation of tasks and admin controls  Alarm management  Validation of procedures  Workload assessment | Review of HF RGP  Data collection and event reporting  Ongoing training and competence management  Review of procedures  Change management |
| Example HMI considerations | Task understanding  Layouts of control room and initial location of instruments (remote HMI)  High-level task analysis  Use case development  System reqs and constraints  Style guide development  Alarm and notification identification and initial rationalisation  Future planning (maintenance, decommissioning, technology advancement, etc.) | Task decomposition  Identification and analysis of all potential errors  Identification and consideration on tasks and layout of performance shaping factors for HMI (e.g., noise levels, lighting in room, shift durations, etc.)  Layout review (link analysis, etc.)  HMI requirements and features in design specifications  Workload and timeline analysis  Style guide further development (e.g., colour / font differences across systems, timings, etc.)  Alarm rationalisation and definitions (system alarms, notifications of HMI errors)  Layout revision based on AoF, HRA, trial outputs, system developments, etc.  Mock-ups / VR / prototyping  Usability and operability  Consideration of procedures and training needs  Future planning (maintenance, decommissioning, technology advancement, etc.) | Compliance with standards and requirements (i.e., RGP, ISO, Style guide, HRA, etc.)  Feed into training programme  Feed into procedure writing  Review of related admin controls  Usability and operability trials | Plant walkdowns  Field trials  ISV trials  Timely alignment with commissioning activities  Data collection to feed into HRA processes | Introduction of new tasks  Change in equipment designs  Change in staffing concept  Ageing and degradation – Impact on maintenance and inspection tasks |

**Notes:**

ONR recognises that many designs are based on existing processes rather than ‘blue sky thinking’. Therefore, some projects will not include all of the system maturity phases outlined here.

The ONR SAPs highlight the need to consider decommissioning early in the project lifecycle. Therefore, this table has not listed this as a separate system maturity phase.

The HF topics listed will persist throughout the project lifecycle and are presented in this table to indicate the point at which they should be considered for maximum effect, thus avoiding design foreclosure in the later phases of system maturity. However, Inspectors must be cognisant of each project context when considering which HF topics are relevant and the timing of HFI and HMI activities.

# Appendix B – Automated and autonomous assistive systems

## Introduction

1. ONR considers automated[[3]](#footnote-4) and autonomous[[4]](#footnote-5) assistive systems (subsequently referred to as assistive systems) to be those that replace or enhance the traditional operator tasks such as detection and analysis of fault conditions, situation assessment, diagnosis and response planning. The guidance presented within this appendix assumes the assistive system is not fully autonomous and the human is required for command and control. It should be remembered that even fully autonomous systems will require some degree of human intervention, for example during the completion of examination, inspection, maintenance and testing activities and therefore some degree of HF consideration is expected for all systems.
2. Advances in technology provide opportunities for increasing use of automation and autonomy for plant control and supporting decision making with new, novel and more flexible types of HMI that involve personnel interaction with plant and process in different ways. The prospect of artificial intelligence (AI) enabled autonomy[[5]](#footnote-6) introduces further opportunities and challenges that could fundamentally change the role of the human. As the role of the human changes and evolves, it is likely that new types of HMIs will be required, which will complement or replace those currently deployed. Examples of assistive systems that may be found on nuclear installations include:
3. Software utilised by personnel for modelling and calculation, including bespoke systems and those that utilise basic office software (e.g. spreadsheets).
4. Off-line expert systems / simulations (digital twins, virtual models, etc.) that can be interrogated to predict future behaviour of a component, system or plant.
5. Electronic procedures and checklists, which include some automatic population of real-time data and calculations, to aid human decision making.
6. On-line automatic diagnosis systems that monitor actual plant conditions and recommend corrective actions.
7. Automated and semi autonomous robotic applications.
8. Autonomous vehicles that follow a route with little or no human action.
9. Potential sources of further guidance on this topic include:

* BS IEC 63435:2023 Nuclear power plants - Control rooms - Operating support system (Draft for public comment)
* PD CEN ISO/TR 9241-810:2022 Ergonomics of human-system interaction. Robotic, intelligent and autonomous systems
* PD ISO/IEC TR 24028:2020 Information technology. Artificial intelligence. Overview of trustworthiness in artificial intelligence
* BS ISO/IEC 23894:2023 Information technology. Artificial intelligence. Guidance on risk management
* PD IEC TR 63468:2023 Nuclear facilities. Instrumentation and control, and electrical power systems. Artificial Intelligence applications
* NHTSA DOT HS 812 555 2018 Human Factors Design Guidance for Level 2 and Level 3 Automated Driving Concepts

1. Given the rapid technology advances in this area, it is not possible to provide inspectors with a definitive suite of guidance since both research and OPEX are still rapidly evolving. Before undertaking any assessment in area, the inspector should seek out current RGP which will inform their work. It is recommended that in doing this, inspectors look at other relevant industries, including the transportation (land, air and sea) and medical sectors, in addition to the more traditional high hazard applications typically considered.

## Understanding the role of the human

1. A holistic approach should be taken to understanding the role of the assistive system within the broader work system and how the human contributes to / supports delivery of organisational goals. The assistive system will not be used in isolation therefore consideration of the wider sociotechnical system is expected.
2. The human’s role within the assistive system should not be restricted to simply compensating for incomplete automation / autonomy. Ideally, the user interaction with the assistive system should result in a more enriched and engaging role for the human. Robust optioneering, which includes consideration of the operator role, should be undertaken.
3. Where assistive systems are used during the completion of human actions and administrative controls necessary for safety, the dutyholder should be able to clearly explain and substantiate the extent to which the system, the human, or a combination of the two, contribute to the delivery of the associated safety function. The inspector may wish to confirm:

* The allocation of function (AoF) is appropriate and is accurately reflected in any assessment of risk (safety cases) – see NS-TAST-GD-064 [4] for further guidance.
* Proportionate task analysis of the complete system (the assistive system and human working together) has been completed to evaluate the demands placed on the human.
* The HMI is designed to reinforce this allocation of function and support the human to deliver safety functions when they are demanded.
* Should the system become unavailable, or fail in some way, the role the human plays in response and recovery is appropriate and supported using alternative means.

1. Assistive systems are typically delivered by highly complex software-based systems, so it is important that any assessment is supported by C&I and Fault Studies inspectors with respect to the substantiation of any reliability claims made on the system by the dutyholder.
2. The use of a classification systems, which describes different levels of automation / autonomy can be helpful in understanding the HF challenges that need to be addressed in the HMI design. The following is proposed by the US NRC NUREG-0711 [17]:

* Manual operation – No autonomy, human performs all tasks – No automated diagnosis.
* Shared operation – Some automation, human performs some tasks with other being automated – System monitors conditions and selects specific indications to display.
* Operation by consent – Some autonomy, human approves actions prior to initiation, human may allow autonomous for very specific situations but remains in command – System monitors conditions and recommends specific actions for operator to take.
* Operation by exception – High autonomy, autonomous under most situations, human required to approve critical actions prior to initiation – System monitors conditions and initiates most control actions automatically unless operator intervenes.
* Autonomous operation – Full autonomy, automation can not normally be disabled, human performs no tasks – System monitors conditions and initiates control actions automatically.

1. The perceptual and cognitive burden associated with monitoring an assistive system, and the associated loss of skill / ability should not be underestimated (when compared to the user performing the task themselves). Likewise expecting the user to be a failsafe and taking over in response to system mis behaviour / failure is also challenging from a HF perspective (as experience from aviation demonstrates). The provision of suitable and sufficient HMI, with associated task design and procedures focused on maintaining appropriate situational awareness, are key to minimising these risks.

## Design principles

1. The following general principles should be applied in the development of assistive systems.
2. The use of assistive systems to support human performance is generally encouraged, especially for tasks that are known to challenge human competence, capability and capacity (e.g. complex calculations, long duration vigilance tasks, etc.).
3. Robust optioneering, which appropriately integrates HF considerations, should be applied – see NS-TAST-GD-058 [3] for further guidance. In the simplest terms, the question to be asked is should, rather than could, an assistive system be used (i.e. balanced view of the overall costs & benefits and not solely the technical feasibility).
4. Where there might be nuclear safety impact from the use of an assistive system, the human should retain overall control and manually initiate / confirm any actions recommended by the assistive system (rather than those actions being automatically initiated with the option for human veto within a defined time window). The user should remain capable of being able to take command in a timely way where the safety case claims that they will do so.
5. A fault / failure / unavailability of the assistive system will not result in a direct challenge to safety / negative safety consequence.
6. Assistive systems should generate clear and unambiguous signals when their performance falls outside predefined acceptance criteria and human intervention is required.
7. The user should not be expected to respond rapidly to a fault / failure / loss of system functionality. This is particularly important for highly automated / autonomous systems where it might take time for the user to establish an appropriate degree of situational awareness.
8. Systems should be appropriately transparent. Transparency relates to the decision process the system has used to derive a specific outcome. A transparent system allows for independent verification of system output.
9. The output of the system should be explainable. Explainability relates to the ability of the system to be able to communicate (in a manner which is understandable to the user) why a specific outcome has been reached.
10. The potential socio-technical impacts of the system should be identified and appropriate risk management / mitigation strategies implemented and maintained. For example, users may become reliant on an effective and reliable assistive system resulting in a degradation of competence over time. Due to the emergent nature of these issues, on going review of the system and its impacts, is recommended.

## Further guidance

1. When considering the implementation / use of assistive systems, the inspector may wish to consider:
2. How decision making regarding the development and use of assistive systems is informed by RGP and OPEX from similar systems in relevant contexts.
3. That assumptions underpinning earlier optioneering remain relevant, appropriate, and valid and that consideration of human capabilities has informed this (i.e. RGP may have evolved significantly in the time it takes to implement an assistive system).
4. The justification that the selected HMI, including hard and soft controls, are appropriate given the tasks and safety functions being delivered.
5. Evidence demonstrating how the design of the HMI meets relevant good engineering and ergonomics practice and is compatible with the dutyholder’s other HMI conventions and operator expectations.
6. The impact that other tasks and potential workplace distractions may have on the users’ ability to monitor the assistive system effectively. It is likely that users’ attention may be diverted (intentionally or unintentionally), particularly if the assistive system has a perceived high reliability. This risk requires management.
7. Claims that an assistive system reduces operator workload are substantiated before human resource is allocated to alternative work following the introduction of a system. There is risk that the secondary tasks become the users main focus resulting in little or no attention being given to the assistive system without an explicit prompt.
8. The impact the assistive system may have on team dynamics and the ability of the group to maintain appropriate and agreed situational awareness of a situation (i.e. each users has their own HMI versus the conventional panel-based HMI which is shared by the team).
9. The process of ‘handback’ to the assistive system in situations where the user has been required to take command of the system (manual choice or response to a system error / fault). Users will need to know when it is safe to attempt ‘handback’ and the likely impact on the system once assistance is restored (e.g. if the system will trip because it does not have access to sufficient valid data to fulfil its role).
10. The measures the dutyholder implements to manage the level of trust users place on the assistance systems (i.e. a level of trust that reflects the true reliability of the system). Too much (i.e. users blindly follow the guidance of the system without independent verification) or too little (i.e. they always ignore the guidance the system provides regardless of its validity), trust can be problematic. Specific attention should be paid to systems where trust is dynamic (i.e. users should have high trust under some conditions but less or no trust under others).
11. That the dutyholder has identified and is able to access personnel with the necessary skills and competence needed to test and maintain the assistive system, noting these may be quite different from those required to support other systems. The dutyholder must be able to function as an intelligent customer for the assistive system and to ensure that any supporting services are provided on a reliable and timely basis.
12. Any ongoing reviews the dutyholder will undertake to understand the performance of the assistive system, how it is being used and the impact of any emergent issues. Such information should be used to confirm the ongoing validity of the risk assessment.
13. When considering the adequacy of a proposed / implemented assistive system HMI, the inspector may wish to consider:
14. How users maintain situational awareness appropriate to the task. Users will need to understand what the assistive system is doing (status and progress), what decisions it is making and the data it is using to inform these processes. This feedback needs to be presented in a manner that is timely, usable and useful for the user.
15. How the system alerts the user to when their attention and / or an input is required. Multi modal cues can be highly effective but should be used sparingly to preserve their impact.
16. When the system makes a recommendation, how the system communicates the option it has selected and those it has rejected / considers less favourable.
17. How the system communicates the favourability of the selected option versus less favoured or rejected options.
18. How the system communicates any uncertainties associated with its recommendations (e.g. if a specific sensor is offline) and how those recommendations may change should new / different data become available (e.g. if data from that sensor became available).
19. How the user can interrogate the system to understand why the selected option is favourable, including the data the system is using to make its judgement.
20. How the user can select an alternative option to the one recommended by the system and any perceived (e.g. risk of financial consequence) or real (e.g. prompts and warnings) inertia the user may experience “going against the system”.
21. When considering the risks associated with failure or degraded assistive system performance, the inspect may wish to consider:

* The provision of suitable back-up systems and demonstrations (e.g. verification and validation activities) that transition to these can be safely and reliably achieved before negative consequences arise.
* How the failure modes of the assistive system will be revealed and clearly presented to the user in a manner which effectively communicates the associated impact on the system’s ongoing operations.
* How users are expected to intervene and what guidance is available outlining their role in ongoing operations and / or recovery activities, including explicit guidance regarding the use of the (degraded / failed) assistive system in fulfilling these duties.
* How user familiarity with back-up systems is maintained (e.g. use as part of frequent tasks, refresher training, exercises, etc.).

1. Situational awareness can be defined as an individual’s mental model of what has happened in the recent past, an accurate current understanding of the present, and the ability to predict what will happen in the immediate future. [↑](#footnote-ref-2)
2. Graphical representations of the plant/systems that emphasise relationships between components (in either a realistic or stylised manner). [↑](#footnote-ref-3)
3. A traditional automated system acts on a specific task according to pre-defined, prescriptive rules. [↑](#footnote-ref-4)
4. Autonomy is typically considered to involve a set of intelligence-based capabilities that allows the system to respond to situations that were not pre-programmed or anticipated (i.e., decision-based responses) prior to system deployment. [↑](#footnote-ref-5)
5. AI systems typically have a higher degree of self governance and self-directed behaviour (than non-AI autonomy) allowing them to operate without external intervention. [↑](#footnote-ref-6)