Office for Nuclear Regulation

ONR GUIDE			
Human Machine Interface			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-059 Revision 5		
Date Issued:	November 2019	**Review Date:**	December 2022
Approved by:	M Richardson	Professional Lead	
Record Reference:	CM9 Folder 1.1.3.978. (2020/265758)		
Revision commentary:	Rev 4: Fit for purpose update Rev 5: Updated Review Period		

TABLE OF CONTENTS

Published 11/19

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established its Safety Assessment Principles (SAPs) (Ref. 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 duty-holders. 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 is one of these guides.

2. PURPOSE AND SCOPE

2.1 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.

2.2 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 to HMI. 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 HMI. As with all guidance, inspectors should use their knowledge and experience in the depth and scope to which they apply the guidance provided.

2.3 HUMAN MACHINE INTERFACES (HMI)

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 The Nuclear Site Licence Conditions (LCs) (Ref. 2) 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.

3.2 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), 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 (e.g. LCs 19 – 22 and 28).

3.3 Regulation 3(1) of The Management of Health and Safety Work Regulations 1999 (Ref. 3) places a legal requirement on duty holders to produce suitable and sufficient risk assessments. 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 dutyholders measures for controlling risk.

4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED

SAPS

4.1 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).

4.2 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 (e.g. site emergency control centres (see 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:

a) provide sufficient, unambiguous information for the operator to maintain situational awareness in all operating modes and in fault and accident conditions (e.g. the behaviour and status of the automated plant control systems);

b) provide a conspicuous early warning of any changes in parameters affecting safety;

c) provide a means of signalling safety system challenges and of confirming that the safety system has initiated and achieved its safety functions;

d) support effective diagnosis of plant deviations; and

e) 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

f) support communication between personnel located in the same or different operating locations, including locations external to the facility or site.

4.3 Closely linked to EHF.7 are SAPs EHF.1 (Integration with design, assessment and management) NS-TAST-GD-058 [Ref.4] and EHF 2 (Allocation of safety actions) NS-TAST-GD-064 [Ref.4], which are essential supporting activities in the design of a safe and operable HMI.

4.4 In addition, SAPs EHF.5 (Task Analysis) NS-TAST-GD-063 [Ref. 4] and EHF. 6 (Workspaces) NS-TAST-GD-062 [Ref. 4] are also relevant.

IAEA SAFETY STANDARDS

4.5 The guidance is also broadly consistent with IAEA standards and guidance. Key relevant IAEA publications are referenced in Section 5 of this TAG.

4.6 The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2014 (Ref. 1) and are recognised by ONR as relevant good practice. They should therefore be consulted, where relevant, by the inspector.

WENRA REACTOR SAFETY REFERENCE LEVELS

4.7 The guidance in this TAG is consistent with WENRA Reactor Safety Reference Levels (Ref. 5):

1. Issue E (Design Basis Envelope for Existing Reactors): E10. Instrumentation and control systems
2. Issue F (Design Extension of Existing Reactors): F34. Ensuring safety functions in design extension conditions
3. Issue LM (Emergency Operating Procedures and Severe Accident Management Guidelines): LM4. Verification and validation
4. Issue O (Probabilistic Safety Analysis (PSA)): O1. Scope and content of PSA

OTHER

4.8 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 in References 6-8.

4.9 The following British and ISO standards (Ref. 9) may also be applicable to the topic of HMI:

1. BS EN IEC 60964:2019 Nuclear power plants. Control rooms. Design
2. BS EN 60965: 2016 Nuclear power plants. Control rooms. Supplementary control room for reactor shutdown without access to the main control room
3. BS IEC 62954:2019 Nuclear power plants. Control rooms. Requirements for emergency response facilities
4. BS EN 61227:2016 Nuclear power plants. Control rooms. Operator controls
5. BS EN 62241:2015 Nuclear power plants. Main control room. Alarm functions and presentation
6. BS IEC 61772:2009 Nuclear power plants. Control rooms. Application of visual display units (VDUs)
7. BS EN IEC 62646:2019 Nuclear power plants. Control rooms. Computer-based procedures
8. BS EN ISO 11064-(All Parts): Ergonomic design of control centres
9. BS EN ISO 9241-(All Parts): Ergonomics of human-system interaction.
10. BS EN 61839:2014 Nuclear power plants. Design of control rooms. Functional analysis and assignment
11. BS EN 61508-2:2010 – Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems.

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

5. ADVICE TO INSPECTORS

Definition of Human Machine Interface (HMI)

5.1 Humans play a key role in the safe and efficient operation of nuclear facilities. Plant and Facility HMI 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 make human-based safety claims (HBSCs) in respect of reliable interventions for monitoring and control of both normal and abnormal conditions.

5.2 HMI are the principal mechanism through which personnel interact with and control the plant and processes. They provide the facilities for this interaction in the form of various instrumentation, displays, alarms and controls. HMI 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 traditional or advanced / computerised 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. HMI need to support all operational states including normal, abnormal and fault conditions.

5.3 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 traditional analogue controls through to systems where the operational control is transmitted via electrical systems through to advanced HMIs which may incorporate some level of automation.

5.4 Traditional analogue HMI 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.

5.5 HMI where control is transmitted via electrical systems include those where a button transmits a signal to open a valve, or the input to a virtual button on a touchscreen is transmitted to a valve via a programmable system).

5.6 Advanced HMI (which are commonly digital) comprise multiple functions and instruments, which are mapped onto (typically) a number of visual display units. Another feature of digitalised HMI is their ability to support high levels of automation and operator assist systems.

5.7 ONR recognises that HMI can take a wide range of formats from traditional analogue to digital technology and regulate their use in a technology neutral way.

5.8 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 Human Factors inspectors.

5.9 When interacting with HMI, personnel are often required to complete two activities.

5.10 The primary task of using the information presented on the HMI and initiating any appropriate control actions.

5.11 Secondary tasks that interface access and manage tasks required to complete the primary task. For traditional 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.

5.12 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.

5.13 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 nuclear licensed site. Most HMI are supported by C&I or mechanical systems. However, there are other examples, like passive indications used to measure levels, 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

5.14 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 HBSCs 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.

5.15 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 HBSCs, and the demonstration of their ergonomic adequacy in-line with relevant good practice to ensure, so far as is reasonably practicable, the effective management of plant safety and delivery of HBSCs.

5.16 Notwithstanding this, all HMI, not just those incorporated into safety systems, should be designed appropriately and comply with relevant good practice. Non safety-related HMI have the potential to impact on HBSCs, 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 reasonably practicable to do so.

5.17 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
- The nature of the human-based safety claims related to the delivery of plant safety functions
- Key operational requirements and targets
- End user characteristics.

5.18 Understanding of these aspects should be incorporated into an effective and integrated through-life process for the design and operation of HMI.

5.19 Inspectors may consider whether:

1. The need for, and level of reliance on, HMI (and operator actions) to perform important safety functions have been justified on ALARP grounds.
2. The dutyholder's incorporation of HMI within a design is demonstrated in an overall design philosophy and approach (NS-TAST-GD-058 (Ref. 4) uses the term 'Concept of Operations' to describe this). This should also specify the main safety and operability targets to be achieved by the HMI system.
3. 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.
4. The dutyholder has proportionally integrated HF / ergonomics relevant good practice into all areas of HMI design. This should not focus solely on the more high profile HMI such as the main control rooms.

5. The HMI design is included as part of the dutyholder's Human Factors Integration (HFI) process (NS-TAST-GD-058 – Ref. 4) which should have clear links to the dutyholder's project, design, engineering and procurement processes.

6. 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.

7. 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.

8. 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.

9. The dutyholder has considered and taken into account the capabilities, characteristics and numbers of the HMI user population, during its specification and design. Relevant good practice 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.

10. 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.

11. There is a clear documented process that demonstrates how the dutyholder has managed and resolved any conflicts and trade-offs associated with HMI e.g. between safety constraints and ergonomics best practice.

12. 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).

13. Allocation-of-function analysis has been used to inform and support the design (and modification) of HMI.

14. The design and operational concept of HMI has been used as input to the development of procedures and operator training needs / competence requirements.

15. The dutyholder has conducted a 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 these 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 (NS-TAST-GD-050).

16. The HMI available to operators supports the demonstration of on-going compliance with operating rules (NS-TAST-GD-35 – Ref. 4), that parameters remain within the safe operating envelope, and the dutyholder has considered matters such as redundancy and diversity for circumstances where HMI is unavailable.

17. The dutyholder has used its design and / or review of HMI to inform the assumptions and claims made in its Human Reliability Assessment (NS-TAST-GD-63 – Ref. 4), associated qualitative and quantitative safety assessments, so confirming that that those assessments remain valid throughout the operation of the system.

18. The dutyholder has provided evidence that the reliability of the HMI is sufficient for the risk importance of the related HBSCs. Consultation with other ONR discipline Inspectors may be required to confirm an appropriate HMI equipment classification.

HMI Design Considerations

5.20 This section provides general advice to the inspector regarding good practice expectations for HMI design. 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. The principal aim of the HMI should be to support reliable task performance of HBSCs identified in the safety case.

5.21 Inspectors may consider whether:

1. The dutyholder has ensured that the design of the HMI provides sufficient and unambiguous information to the operator to maintain situational awareness[1] in all plant states (NS-TAST-GD-64 – Ref. 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.

2. 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.

3. 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.

4. 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.

[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.

5. 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 (e.g. loss of or corrupted data) are revealed and not likely to exacerbate fault conditions by misleading operators or making responses difficult.

6. The dutyholder is able to demonstrate that suitable and sufficient alternative or back-up HMI are available to cope with HMI failures. 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:

   a. Where elements of the primary HMI have failed, including where the user has to work from back-up HMI.

   b. In degraded work environments or when Personal Protective Equipment (PPE) must be worn.

   c. How authority is passed from control station to control station or operator to operator.

7. 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.

8. 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.

9. 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.

10. 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 HBSCs.

11. Required control actions and corresponding feedback / response communicated via HMI is consistent across the site / facility and compatible with operator expectations.

12. Where possible, end user representatives have been involved throughout the entire design lifecycle of the HMI.

Overview Screens and Mimic Display Considerations

5.22 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 a 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 traditional panel-based interfaces to display process information. Desktop screen-based systems, that display information to single users, may also be used.

5.23 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.

5.24 It is important that overview displays are designed to support the level of decision-making that they will be used for, as during abnormal or emergency situations they can become the focal point of the operations team.

5.25 Inspectors may consider whether:

1. 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 normal HF / ergonomics good practice and are compatible with other HMI in the plant.

2. 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.

5.26 Mimics[2] 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 (e.g. different mimics for normal operations, shutdown, specific fault /emergency conditions, etc.).

5.27 Inspectors may consider whether the duty holder has provided a rationale for the style (e.g. task versus plant-based displays) and the degree of detail on any mimics including the specification of conventions to be applied.

Emergency Shutdown (ESD) / Post Accident Monitoring (PAM) Considerations

5.28 The main purpose of 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 PAM HMI should provide the capability to monitor parameters that are needed for incident management purposes. These may include temperature, reactivity, pressure, and safety system activation status.

5.29 Inspectors may consider whether:

1. 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 (e.g. fire, flood, seismic activity, etc.).

2. 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.

[2] Graphical representations of the plant / systems that emphasise relationships between components (in either a realistic or stylised manner)

3. Where reasonably practicable, the use of the HMI has been tested/exercised in a high-fidelity simulation to demonstrate its effectiveness (e.g. 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

5.30 Although communication system design is too complex to cover within the scope of this TAG, there are a number important issues for the inspector to consider that relate to HBSCs underpinned by reliable communication:

1. Where communications equipment is key to achieving a safe stable state, it needs to remain available under the anticipated fault conditions.

2. 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.

3. The information needing to be transmitted.

4. To whom it needs transmitting.

5. When it needs to be transmitted (e.g. is information needed immediately).

6. The clarity with which the information needs transmitting.

7. What the receiver will be expected to do with the information.

5.31 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.

5.32 Inspectors may consider whether:

1. 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.

2. 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, and emergency activities. Where possible this should be tested / exercised under realistic conditions.

3. 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.

4. The dutyholder has produced a communications plan detailing how the system/s will be used.

Control Room / Control Centre Design Considerations

5.33 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 NS-TAST-GD-62 (Ref. 4) 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.

5.34 Inspectors may consider whether:

1) 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.

2) 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, is adequate space provided for the plant and instrumentation drawings, or hard-copy procedures to be viewed? 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?

3) Where the dutyholder proposes to have multiple control rooms (e.g. 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 and the HMI they house, are consistent with good ergonomic practice and conventions used elsewhere in the site / facility HMI.

4) The dutyholder has considered all appropriate environmental human factors issues for all foreseeable plant states. Post event habitability is a key area of interest.

Automation / Computerised Support System Considerations

5.35 Advances in digital technology are enabling the increasing use of automation for plant control and supporting decision making with new and more flexible types of HMI that involve personnel interaction with plant and process at varying levels. These include, for example, the introduction of operator assist systems such as automatic diagnosis.

5.36 ONR considers automated / computerised support 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.

5.37 These features are typically delivered by highly complex software based systems, so it is important that any assessment is supported by Control & Instrumentation (C&I) and Fault Studies inspectors with respect to the substantiation of any reliability claims made on the system by the dutyholder.

5.38 It is important that the dutyholder properly understands how the associated safety function is delivered and to what extent reliance is placed on the system, the operator, or a combination of the two. The HMI should then be designed to support/reinforce this allocation of function.

5.39 Examples of automated / computerised support HMI include:

1. Advanced Controls that combine multiple control methods and are based on screen-based operation, where the operator actions are mediated by computer systems.

2. Computerised operator support systems that run real-time simulations of plant state to support operator diagnosis and decision-making.

3. Intelligent agents that perform information processing tasks for operators in an autonomous manner, e.g. Automatic Diagnosis.

4. Computer-based procedures that may incorporate monitoring, control and decision-making capability.

5. Synthetic plant models, against which real plant data can be compared.

6. Control suites where information can be displayed dynamically across a number of monitors in a display and through enhanced auditory signals.

5.40 Automated/computerised HMI may be found across a nuclear facility, both within control rooms and across local plant. For example, a spread sheet used in an office to decide which stored fuel elements are suitable for a specific subsequent process may be considered an automated/computerised support HMI if there are no subsequent independent checks using independent data, that can be made to verify the decision making process. Automated/computerised HMI of this type may attract safety classifications and it is important that these are substantiated wherever the HMI are located.

5.41 Inspectors may consider whether :

1. The dutyholder's choice of automated / computerised support HMI is appropriate given the tasks and safety functions being delivered.

2. The design of automated / computerised support HMI meets relevant good engineering and ergonomic practice and is compatible with the dutyholder's traditional HMI conventions and operator expectations.

3. The dutyholder has provided suitable back-up systems should automated/computerised support HMI fail and has demonstrated that transition to these can be safely and reliably achieved. This includes adequate provision for back-up of safety critical parameters should computerised/advanced displays and controls fail or corrupt.

4. The dutyholder can demonstrate that the failure modes of automated / computerised support displays and controls will be revealed, clearly presented to the operator and that the associated impact on the system's operation and understanding of the plant processes is properly understood. It should be clear when (or if) operators are expected to intervene and what guidance will be available outlining the operator's role in operations / recovery activities, include the use of the (potentially failed) HMI in fulfilling these duties.

5. The dutyholder can demonstrate that any soft-control implementation is suitable for the type of control actions required.

6. The dutyholder can demonstrate that any automated / computerised support HMI design is compatible with the user capabilities and competencies.

7. Where automated systems are proposed or being used, the dutyholder has ensured that adequate feedback is provided to operators informing them of what the automated system is doing, including its status and progress (i.e. the decisions it is making and the information it is using to inform these processes).

8. The design and implementation of any automated/computerised support HMI and automated process control system proposed by the dutyholder ensures that the operator will remain capable of being able to take command of plant and processes being operated where the safety case claims that they will do so.

9. The dutyholder has considered the implications for team dynamics and maintaining situational awareness when considering the design and implementation of computerised HMI and computer-based procedures.

10. The dutyholder has demonstrated as part of its verification and validation activities that sufficient HMI functionality remains operable to maintain the plant in a safe state and to deliver the required safety functionality in the event of automation failures.

Alarm System Considerations

5.42 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.

5.43 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. These should be separate to the alarm system where reasonably practical.

5.44 ONR recognise The Engineering Equipment & Materials Users' Association (EEMUA) 191 guide (Ref. 10) as relevant good practice for alarm design and management. Inspectors are referred to this reference for comprehensive guidance on the design, implementation and assessment of alarm systems.

5.45 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 well documented by the dutyholder.

5.46 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). Key expectations for an alarm system are listed below.

5.47 Inspectors may consider whether:

1. The dutyholder has an alarm design and management strategy document, which includes an overall philosophy for the design and management of alarm systems.

2. The dutyholder has justified the need for, and properly engineered its alarm systems within its overall HMI.

3. 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.

4. 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.

5. All safety-related alarms, their settings and priorities are presented in a quality controlled alarm schedule or similar document.

6. The dutyholder can demonstrate that required responses to alarms are supported by suitable alarm response instructions.

7. 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 EEMUA 191 (Ref. 10) (or equivalent), which limits the amount of risk reduction that can be claimed using alarms.

8. The dutyholder's alarm system meets with general ergonomic good practice expectations for HMI.

9. 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 EEMUA 191 (Ref. 10).

HMI Modernisation Considerations

5.48 The IAEA (Ref. 11) states that there are a number of specific issues that need to be considered during the modernisation of existing HMI:

1. It may be necessary to reconstruct the design basis of the plant.

2. Even with an existing design basis, it may be necessary to interpret its requirements for digital C&I.

3. Compromises may have to be made because the project has to adapt to the existing plant and its operational requirements.

5.49 The key HF issues associated with 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 human factors / ergonomics good practice. Even in instances where the conventions are compatible, there will considerable training and procedural overheads associated with such a project.

5.50 Inspectors may consider whether:

1. The dutyholders HMI modernisation project is being carried out in line with the expectations for a new build.

2. 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 modernisation decisions and their impact should be clearly reflected in the dutyholder's safety case and Human Reliability Analysis (HRA) and demonstrated to reduce risks to ALARP.

3. The dutyholder has assessed the risks associated with the transition from the extant HMI to the 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.

6. REFERENCES

1. ONR Safety Assessment Principles for Nuclear Facilities 2014 Edition Revision 0
2. ONR Licence condition handbook February 2017
3. The Management of Health and Safety at Work Regulations 1999
4. ONR TAGs
    a. NS-TAST-GD-058 Human Factors Integration
    b. NS-TAST-GD-064 Allocation of function between human and engineered systems
    c. NS-TAST-GD-063 Human Reliability Analysis
    d. NS-TAST-GD-062 Workplaces and work environment
    e. NS-TAST- GD-035 The Limits and Conditions for Nuclear Safety (Operating Rules)
5. WENRA (2014) Safety Reference Levels for Existing Reactors
6. NUREG 0700 (2002), Human-System Interface Design Review Guidelines
7. DEF-STD 00-251: Human Factors Integration for Defence Systems - Part 3: Human Factors System Requirements
8. EEMUA Publication 201 (2010) Process plant control desks utilising human-computer interfaces: a guide to design, operational and human-computer interface issues
9. British / ISO standards
    a. BS EN IEC 60964:2019 Nuclear power plants. Control rooms. Design
    b. BS EN 60965: 2016 Nuclear power plants. Control rooms. Supplementary control room for reactor shutdown without access to the main control room.
    c. BS IEC 62954:2019 Nuclear power plants. Control rooms. Requirements for emergency response facilities
    d. BS EN 61227:2016 Nuclear power plants. Control rooms. Operator controls
    e. BS EN 62241:2015 Nuclear power plants. Main control room. Alarm functions and presentation
    f. BS IEC 61772:2009 Nuclear power plants. Control rooms. Application of visual display units (VDUs)
    g. BS EN IEC 62646:2019 Nuclear power plants. Control rooms. Computer-based procedures
    h. BS EN ISO 11064-(All Parts): Ergonomic design of control centres
    i. BS EN ISO 9241-(All Parts): Ergonomics of human-system interaction.
    j. BS EN 61839:2014 Nuclear power plants. Design of control rooms. Functional analysis and assignment

k. BS EN 61508-2:2010 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems

10. EEMUA Publication 191 (2013) Alarm systems - a guide to design, management and procurement

11. IAEA Nuclear Energy Series, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants

7. GLOSSARY AND ABBREVIATIONS

ALARP	As low as reasonably practicable
C&I	Control and Instrumentation
EEMUA	Engineering and Equipment Materials Users' Association
ESD	Emergency Shutdown
HBSC	Human Based Safety Claim
HF	Human Factors
HFI	Human Factors Integration
HMI	Human Machine Interface
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
LC	Licence Condition
ONR	Office for Nuclear Regulation
PAM	Post Accident Monitoring
PFD	Probability of Failure on Demand
PPE	Personal Protective Equipment
PSA	Probabilistic Safety Analysis
RPE	Respiratory Protective Equipment
SAP	Safety Assessment Principle
SFAIRP	So far as is reasonably practicable
TAD	Target Audience Description
TAG	Technical Assessment Guide
UK	United Kingdom
VDU	Visual Display Unit
WENRA	Western European Nuclear Regulators' Association