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 3		
Date Issued:	November 2016	**Review Date:**	November 2019
Approved by:	E Vinton	Professional Lead	
Record Reference:	TRIM Folder 1.1.3.776. (2016/439734)		
Revision commentary:	Routine update		

TABLE OF CONTENTS

Published 11/16

1. INTRODUCTION

1.1 ONR has established its Safety Assessment Principles (SAPs) 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), specifically SAPs, ESS 3, ESR 1 and EHF.7. 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 am experienced Human Factors 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 ALARP 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)

2.4 Humans play a vital role in the safe and efficient operation of nuclear facilities. Human actions (or inactions) that fail to achieve what should be done in a given situation can be important contributors to facility risk. 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 in respect of reliable interventions for monitoring and control of both normal and abnormal conditions.

2.5 HMIs 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.

2.6 There are no hard and fast definitions for these different types of HIMs, instead it makes more sense to consider them on a continuum. Traditional analogue controls at one extreme that feature one-to-one mapping of function to control (e.g. a hand-wheel which is used to open and control a valve); through the various means via which the operation of a control is transmitted into action via electrical systems (e.g. a button transmits an signal to open a valve, or the input to a virtual button on a touchscreen is transmitted to a valve via a programmable system); to advanced HMIs where multiple functions are mapped to a smaller number of controls/displays by the use of automation control which do not always feature the same spatial dedication (e.g. a virtual button on a touchscreen the function of which changes depending on the current context of use).

2.7 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.

2.8 When interacting with HMIs, 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 traditional HMIs, 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.

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.

2.9 HMIs are generally 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 HMIs are supported by with C&I or mechanical systems however others for example, static gauges used to measure levels, 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.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 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.

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 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, IAEA AND OTHER SAFETY STANDARDS

4.1 SAPS

4.2 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, ESR 7 & 8), Human Factors (EHF 1–12) and Containment and Ventilation (ECV. 6 and 7).

4.3 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.

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

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

4.6 IAEA SAFETY STANDARDS

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

4.8 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.

4.9 WENRA REACTOR SAFETY REFERENCE LEVELS

4.10 The guidance in this TAG is consistent with WENRA Reactor Safety Reference Levels:

- Issue E (Design Basis Envelope for Existing Reactors): E10. Instrumentation and control systems
- Issue F (Design Extension of Existing Reactors): F34. 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

4.11 OTHER

- 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 which ONR recognises as sources of relevant good practice are provided in Refs 1-1.

4.12 BS EN 61508-2:2010 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems may also be an applicable standard for the design of HMIs, covering all lifecycle aspects.

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

5. ADVICE TO INSPECTORS

5.1 INTRODUCTION

5.2 This TAG provides guiding principles to inform inspectors' expectations regarding how a dutyholder will demonstrate that HMI provisions will support effective human performance. In particular, those expectations regarding the dutyholder's demonstration of the feasibility of delivering Human-Based Safety Claims (HBSCs) and reducing risks so far as is reasonably practicable. The guidance provided in this section is applicable to the assessment of all types of HMI.

5.3 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 HMI. Inspectors should have confidence that the dutyholder's process adequately identifies the need for 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.

5.4 Notwithstanding this, all HMIs, not just those incorporated into safety systems, should be designed appropriately and comply with relevant good practice. None safety-related HMIs have the potential to impact on HBSCs, either by being located in close proximity to safety-related HMIs or by communicating similar information. HMI-general expectations

5.5 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, and
- end user characteristics.

5.6 These understandings should be incorporated into an effective and integrated through-life process for the design and operation of HMI.

5.7 Inspectors may consider whether:

1) The need for and level of reliance on HMIs (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 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.

3) The dutyholder has used its safety case to specify requirements and a proportionate level of task analysis to inform the design (and modification) of HMI.

4) The dutyholder has integrated human factors/ergonomics best practice in all areas of HMI design and not just focussed on the more high profile HMI such as the control rooms. The HMI design is included as part of the dutyholder's Human Factors Integration (HFI) process (NS-TAST-GD-058) which should have clear links to the dutyholder's project, design, engineering and procurement processes.

5) 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 underlying the design. The style guide describes the design principles, standards and conventions to be applied in the HMI design. Note that where non-UK standards are proposed/used the dutyholder has considered any differences in conventions which are contrary to UK good practice standards.

6) Where dutyholders develop and adopt in-house standards on the design and layout of HMI, the dutyholder has clearly set out the standards and guidance proposed/used and justified them to extent that ONR inspectors can judge them relevant good practice when viewed against the SAPs and this TAG.

7) 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.

8) The dutyholder has considered and taken into account the capabilities, characteristics and numbers of the target users who will be available to use the HMI, during its specification and design. Relevant good practice is for such information to be presented in a Target Audience Description (TAD) document. This avoids unsubstantiated assumptions about end users of the HMI being made throughout the design process.

9) 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.

10) 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.

11) 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).

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

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

14) The dutyholder has conducted a suitable human factors /ergonomics evaluation and testing/trials of the design, development and use of HMI and that this has

demonstrated that the HMI is effective in the context of the design philosophy and safety case claims and assumptions. It is expected such evaluation is undertaken throughout the system lifecycle, for example as part of periodic safety review (NS-TAST-GD-050).

15) The HMI available to operators supports the demonstration of on-going compliance with operating rules (NS-TAST-GD-35), 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.

16) 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), associated qualitative and quantitative safety assessments, so confirming that that those assessments remain valid throughout the operation of the system.

17) The dutyholder has addressed the issue of the safety integrity level requirements of the data display upon which the operator is required to respond. The C&I discipline inspector should be consulted on these issues.

5.8 HMI DESIGN EXPECTATIONS

5.9 This section provides general advice to the inspector regarding good practice expectations for HMI. 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, in all anticipated conditions, and moreover, facilitates the achievement of the HBSCs identified in the safety case.

5.10 Inspectors may consider whether:

1) The dutyholder has ensured that the design of the HMI (whether traditional or advanced) provides sufficient and unambiguous information to the operator to maintain situational awareness[1] in all plant states (NS-TAST-GD-64). 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 the purpose in order to reduce errors and response times.

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.

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

[1] Situational awareness can be defined as an individual's mental model of what has happened, the current status of the system, and what will happen in the next brief time period.

likely to exacerbate fault conditions by misleading operators or making responses difficult.

6) The dutyholder is able to demonstrate that adequate functionally redundant HMI exists to cope with failures of the primary HMI and that this (secondary) HMI has been developed following the same design philosophy. It should be confirmed that the dutyholder has specifically considered how the HMI will be operated under sub-optimal conditions. For example, where elements of the primary HMI have failed and the user has to work from back-up HMI, degraded work environment or when significant personal/ respiratory protective equipment (PPE / RPE) must be worn. Issues such as how authority is passed from control station to control station or operator to operator have been considered.

7) The dutyholder has considered the impact of inadvertent activation of controls and has designed the HMI to 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 responses are consistent across the site/facility and with operator expectations.

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

5.11 OVERVIEW SCREEN(S) AND MIMICS

5.12 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, computer-generated HMIs are being used instead of more traditional panel-based interfaces to display detailed process information. Desk-based systems, that display information to single users, may also be used.

5.13 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, facilitate the development of a common understanding of plant conditions.

5.14 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.

5.15 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 human factors / ergonomics good practice and are compatible with other HMIs 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, as required, in order to detect and correct errors or to lend prompt support where required.

5.16 Mimics[2] are also used as operator support tools, which encourage operators to form accurate mental models of system functions. However, they need to be designed carefully to ensure that the operator can accurately understand the processes and functions to which the mimic relates. The manner in which mimics are laid out is often the basis of the users understanding of the system and can significant 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.).

5.17 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.

5.18 EMERGENCY SHUTDOWN (ESD) / POST ACCIDENT MONITORING (PAM) HMI

5.19 The main purpose of Emergency Shutdown / Post Accident Monitoring HMI is to enable the operator to maintain plant safety, where the conditions of the incident permit and, where they do not, to monitor a set of system parameters that are needed for incident management purposes. For example, these may include; temperature, reactivity, pressure, safety system activation status, etc.

5.20 Inspectors may consider whether:

1) Emergency Shutdown / Post Accident Monitoring HMI are consistent with good practice HMI design expectations and with other relevant HMI across the site / facility and has been 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 which demonstrates that the HMI, including HMI at emergency locations, provides all the necessary plant status information and control functionality needed by an emergency response / management team to implement their emergency response plan.

3) Where possible, the use of the HMI has been tested/exercised in a simulation that is as real as is reasonably practicable to demonstrate its effectiveness (e.g. wearing of anticipated PPE / RPE, limited illumination, smoke, etc.).

5.21 COMMUNICATIONS SYSTEM DESIGN PRINCIPLES

5.22 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 which relate to HBSCs involving communication:

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

- where the equipment is needed to transmit / receive the information, and under what circumstances it needs to remain available
- the potential alternative communication channels available (i.e. verbal and non-verbal) and where they are located relative to the task(s) being performed,
- the information needing to be transmitted
- to whom it needs transmitting,
- when it needs to be transmitted (e.g. is information needed immediately),
- the clarity with which the information needs transmitting,
- what the receiver will be expected to do with the information,

5.23 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.

5.24 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.

5.25 CONTROL ROOM / CONTROL CENTRE DESIGN

5.26 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] 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.

5.27 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.

5.28 AUTOMATION / COMPUTERISED SUPPORT

5.29 Advances in digital technology are resulting in 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. ONR considers automated / computerised support HMIs to be any system that performs traditional operator tasks such as detection and analysis of fault conditions, situation assessment, diagnosis and response planning, independent of personnel. In addition to consideration of the adequacy of the human factors associated with automated / computerised support HMI, inspectors should ensure that the relevant C&I discipline inspectors are consulted with respect to the substantiation of any reliability claims made on the system by a dutyholder. It is particularly 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.

5.30 Examples of automated / computerised support HMI include :

- Computer-based procedures which may incorporate monitoring, control and decision-making capability.
- Computerised Operator Support Systems that run real-time simulations of plant state to support operator diagnosis and decision-making.
- Intelligent Agents that perform information processing tasks for operators in an autonomous manner.
- Control suites where information can be displayed dynamically across a number of monitors in a display and through enhanced auditory signals.
- Advanced Controls that combine multiple control methods and are based on screen-based operation, where the operator actions are mediated by computer systems.

5.31 Automated / computerised support HMIs may be found in control rooms and across a nuclear facility. For example, a spreadsheet 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.

5.32 Inspectors may consider whether :

1) The dutyholder's choice of automated / computerised support HMI is appropriate for the tasks and safety functions to be delivered.

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

3) The dutyholder has given consideration to the provision of, and feasibility of a means of transition to back-up systems should automated/computerised support HMI fail. 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 acceptable to the end users and is compatible with their 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 (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.

5.33 ALARM SYSTEMS

5.34 Alarms and alarm systems often form an integral aspect of a 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 faults. The Engineering Equipment & Materials Users' Association (EEMUA) 191 is recognised by ONR 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.

5.35 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 thus 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.

5.36 The key point is that 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 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.

5.37 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.

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 apply the relevant good practice contained in EEMUA 191, which limits the amount of risk reduction which can be claimed using alarms[3,4].

8) The dutyholders 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.

5.38 HMI MODERNISATION CONSIDERATIONS

5.39 The IAEA [REF] states that there are a number of specific issues that need to be considered during the modernisation of existing HMI:

[3] EEMUA 191 recommends that where an alarm system is considered to be safety-related, the probability of failure on demand (PFD_{avg}) of the overall safety function must be lower than 0.1.
[4] EEMUA 191 states that even where the time to respond is long, or there are multiple alarms or the alarm response is relatively simple, that in no circumstances should a PFD_{avg} of less than 0.01 for any safety function which requires an operator action in response to an alarm.

- It may be necessary to reconstruct the design basis of the plant;
- Even with an existing design basis, it may be necessary to interpret its requirements for digital C&I;
- Compromises may have to be made because the project has to adapt to the existing plant and its operational requirements

5.40 The key human factors 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.

5.41 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 contravene current human factors/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 dutyholders safety case and 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 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. BS EN ISO 11064−1:2001 Ergonomic design of control centres - Part 1: Principles for the design of control centres
2. BS EN 62241:2015 Nuclear power plants. Main control room. Alarm functions and presentation
3. BS EN 60964:2010 Nuclear power plants. Control rooms. Design
4. BS EN 61772:2013. Nuclear power plants. Control rooms. Application of visual display units (VDUs)
5. BS IEC 62646:2012. Nuclear power plants. Control rooms. Computer based procedures
6. BS EN 61227:2016 Nuclear power plants. Control rooms. Operator controls
7. BS EN ISO 9241-210:2010 Ergonomics of human-system interaction Part 210: Human-centred design for interactive systems
8. NUREG 0700 (2002), Human-System Interface Design Review Guidelines
9. DEF-STD 00-251: Human Factors Integration for Defence Systems - Part 3: Human Factors System Requirements
10. EEMUA Publication 191 (2013) Alarm systems - a guide to design, management and procurement
11. EEMUA Publication 201 (2010) Process plant control desks utilising human-computer interfaces: a guide to design, operational and human-computer interface issues

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
HFI	Human Factors Integration
HMI	Human Machine Interface
IAEA	International Atomic Energy Agency
LC	Licensee Condition
ONR	Office for Nuclear Regulation
PAM	Post Accident Monitoring
PFD	Probability of Failure on Demand
PPE	Personal Protective Equipment
PSA	Probabilistic Safety Analysis
PSR	Periodic Safety Review
RPE	Respiratory Protective Equipment
SAP	Safety Assessment Principle(s)
SFAIRP	So far as is reasonably practicable
SSC	Structure, System and Component
TAD	Target Audience Description
TAG	Technical Assessment Guide(s)
UK	United Kingdom
VDU	Visual Display Unit
WENRA	Western European Nuclear Regulators' Association