| **Workspaces, Equipment and User Interfaces** | | | |
|---|---|---|---|
| **Doc. Type** | ONR Technical Assessment Guide (TAG) | | |
| **Unique Doc. ID:** | CNS-TAST-GD-3.3 | **Issue No.:** | 3 |
| **Record Reference:** | 2022/14820 | | |
| **Date Issued:** | Apr-22 | **Next Major Review Date:** | Apr-27 |
| **Prepared by:** | | Principal Inspector | |
| **Approved by:** | | Superintending Inspector | |
| **Professional Lead:** | | Superintending Inspector | |
| **Revision Commentary:** | Major update to align with updated SyAPs. | | |

## Table of Contents

# 1. Introduction

1. ONR has established its assessment principles, which apply to the assessment by ONR specialist inspectors of safety, security and safeguards submissions for nuclear facilities or transports that may be operated by potential licensees, existing licensees, or other dutyholders. These assessment principles 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 against all legal provisions applicable for assessment activities. This technical assessment guide (TAG) is one of these guides.

2. The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 ('NISR 2003') [1] may also use the ONRs Security Assessment Principles (SyAPs) [2] as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This TAG is such a guide.

# 2. Purpose and Scope

3. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's workspaces, equipment and user interfaces. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

# 3. Relationship to Relevant UK Legislation and Policy

4. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

5. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.

6. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve SyDP 3.3 – Workspaces, equipment and user interfaces, in support of FSyP 3 – Management of Human Performance. The TAG is consistent with other TAGs and associated guidance and policy documentation.

7. The Government Functional Standard on security [3] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties. The security principles, governance, life cycle and practices detailed within the Functional Standard have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.

8. The Government Security Classifications document, together with the ONR Classification Policy [4] describes types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

# 4. Relationship to International Standards and Guidance

9. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [5] and the IAEA Nuclear Security Fundamentals [6]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.

10. Fundamental Principle E of the CPPNM refers to the responsibility of dutyholders to implement a Physical Protection System (PPS). It details that the State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorising documents. The importance of physical protection of Nuclear Material (NM) and Other Radioactive Material (ORM) is also recognised in the Nuclear Security Fundamentals, specifically Essential Element 3: Legislative and Regulatory Framework – 3.3 The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime should provide for the establishment of systems and measures to ensure that NM and ORM are appropriately accounted for or registered and are effectively controlled and protected.

11. Fundamental Principle I of the CPPNM refers to the concept of several layers and methods of protection (structural or other technical, personnel and organisational) afforded by the PPS. A more detailed description of the graded approach is provided in Recommendation's level guidance, specifically Nuclear Security Series (NSS) 13 [7]. This document states that dutyholders should prepare a security plan based on a threat assessment or the design basis threat and should include sections dealing with design, evaluation, implementation, and maintenance of the PPS. Sections 4, 5 and 6 contain more detailed guidance on specific measures that dutyholders should adopt to protect NM/ORM against theft and sabotage.

12. The importance of issues relating to human performance are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12:

  d) Allocating sufficient human, financial and technical resources to carry out the organisation's nuclear security responsibilities on a continuing basis using a risk informed approach; and

  e) Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the nuclear security systems.

13. A more detailed description of the elements is provided in Recommendation's level guidance [7]. This publication highlights the importance of designing robust Physical Protection Systems including engineered and operational

security measures, evaluating and demonstrating their effectiveness. It also highlights the importance of ensuring integrated solutions that manage the interface with safety systems to avoid adverse impact and to ensure they are mutually supportive.

# 5. Advice to Inspectors

14. Humans play a key role in the delivery of nuclear security, forming an integral part of the protective security arrangements. Where tasks are undertaken by people in support of nuclear security, the task environment in which they are undertaken should be designed and managed to maximise human performance and minimise the likelihood of human failure.

15. The task environment in which nuclear security tasks are completed is comprised of a number of elements. This includes workspaces, such as security control centres, the physical environment, both indoors and outdoors, as well as the equipment, and Human Machine Interfaces (HMIs) used to monitor the security environment, determine what security actions are required and carry them out successfully. Good design and/or procurement of security infrastructure to be operated by people is dependent on an integrated consideration of all elements of the task environment in order to promote situational awareness, vigilance and decision making.

16. Whilst it will often be the case that a synergy will exist in the requirements for the design of workspaces, the environment and equipment to achieve safety and security goals, it should be recognised that there may be occasions when these requirements are in competition. For example, for safety it may be beneficial to allow staff to readily access parts of the site where safety actions are required or to access sources of information to support decision making. For security however, it may be necessary to restrict the flow of personnel by the design of access barriers, the need to confirm the identity of personnel and to restrict access to information and materials e.g., by the use of passwords or key control arrangements. In such cases, inspectors will need to be sensitive to the potential conflicts between security and safety requirements when undertaking assessment of the adequacy of a dutyholder's task environments. This will require inspectors to consider all requirements on people in a holistic way, taking a balanced, structured and transparent approach to the impact of the task environment on different types of risk.

17. In order to ensure that the task environment is appropriately designed to maximise human performance it is important that tasks are analysed and understood. The design of workspaces, equipment and HMIs should be shown to meet the needs of the users with the depth of analysis undertaken being proportionate to their importance in delivering the necessary security functions. This can be achieved both by desk top analysis and by various forms of testing in order to provide evidence of personnel's ability to deliver security outcomes relied upon in the dutyholder's security plan and supporting documentation.

18. This TAG informs regulatory assessment of the management of human performance and addresses the aspects of workspaces, equipment and user interfaces. Whilst the focus in this TAG is on security important tasks and the achievement of security functions, the principles expressed within apply

proportionately to all aspects of the task environment not only those supporting security important tasks. The design of the task environment should be undertaken in a manner which integrates human factors principles and guidance in a structured manner.

19. The process of designing a task environment to maximise human performance involves the application of good ergonomic practice. This is often referred to as fitting the task to the person and is exemplified by a process known as user centred design. Ergonomics is a core discipline in the field of human factors and provides many detailed principles, standards and guidance relating to the design and specification of workspaces, equipment and user interfaces. These are considered too numerous and specific to include within a TAG, rather this document provides high level guidance on the topics and issues an inspector should consider when evaluating aspects of a dutyholder's security plan and supporting documentation relevant to this area.

20. This guidance should be applied in a proportionate and targeted manner at each stage of a system's lifecycle. The emphasis that the inspector gives to assessing the suitability of a dutyholder's arrangements for the design of elements of the task environment will depend upon the plan being assessed and graded approach. For example, where workspaces, equipment and user interfaces are already well established and there is good evidence of successful performance using them, it may not be necessary to closely scrutinise the process by which they are designed. Conversely, where new workspaces e.g., a new control room or new technology is being introduced then closer scrutiny of the arrangements for the design, development and testing of these may be warranted. As an overriding principle, the inspector should consider the security significance (as affected by aspects including security function category or the categorisation for theft or sabotage) of the activities concerned and the level of reliance on the human for the delivery of security and adopt a proportionate and targeted approach to applying the guidance in this document.

21. As a general principle, where the assessment of a dutyholder's task environment identifies shortfalls in provision against RGP, an inspector should consider the likely impact of this shortfall when making regulatory judgements. For example, if an element of the task environment is found to be deficient the impact of this may be small if the element is used infrequently, the system it is found within plays only a small role in the achievement of nuclear security and there is clear evidence that the task is achievable. In such cases it may be acceptable for the dutyholder to acknowledge the shortfall and present a coherent argument that no change to the task environment is required, particularly where such change may be costly, have significant impact on the way in which tasks that are clearly achievable are undertaken and introduce a significant burden in terms of re-training or procedural updates.

# 6. Regulatory Expectation

22. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies how they adopt a systematic approach in order to provide suitable and sufficient workspaces, equipment and user interfaces to support people in the delivery of nuclear security.

| | | |
|---|---|---|
| **FSyP 3 – Management of Human Performance** | Suitable and Sufficient Workspaces, Equipment and User Interfaces | SyDP 3.3 |
| Suitable analysis should be undertaken to demonstrate that workspaces, equipment and user interfaces are designed to match human capabilities, support reliable human performance and delivery of security functions. | | |

# 7. Workspaces

23. Workspaces in which tasks important for security are completed should be designed taking proportionate account of the capabilities, characteristics and numbers of the intended users and the operational requirements relevant to the workspace where tasks are undertaken. In designing workspaces dutyholders should consider any requirements for the wearing and storage of PPE and use of tools and equipment. Dutyholders should demonstrate that the physical arrangement of the workspaces (internal and external) have taken account of, and are compatible with, human perceptual (vision, hearing) and physical characteristics (reach, strength, dexterity) and limitations, as well as task demands, attributes and characteristics, and the need for communication and interaction between staff.

24. Workspace design should ensure that operators have sufficient space to carry out all tasks important to security under all conditions. This should include provision for any mobile equipment that is necessary to support a task and consider all tasks performed in an area including maintenance tasks as well as normal security tasks. When considering the adequacy of the dimensions of the workspace, designers should consider the likely numbers of people that may need to travel through individual work areas and corridors, doorways, stairways etc. and recognise that these numbers may change e.g., in response to security events where a large number of people may need to travel to the site of a security event in a short space of time. The design of the workspace should be based on the most demanding scenarios which require the largest number of people to assemble in the shortest times, e.g., to facilitate mustering.

25. Whilst normally safety and security requirements for the design of workspaces will be complimentary, it should also be recognised that there is potential for conflict between the two sets of requirements. For example, a security requirement may minimise the number of entry points to a specific area of plant, whilst safety may place a requirement for a greater number of access points to provide alternative egress points in response e.g., to a criticality incident. Similarly, safety may place requirements for easy egress or access to a facility e.g., using crash doors, whilst security is more likely to require access or egress to be more controlled e.g., by using turnstiles and access control systems such as electronic pass readers. A balanced and transparent approach to requirements for different goals will need to be shown by dutyholders and this approach will need to be assessed by security and safety inspectors in a joined-up manner.

26. As well as considering the number of people, the design of the workspace should consider factors such as the likely dimensions and strength of users and issues such as lines of sight. This is known as anthropometrics and it is good practice that the workspace is deigned such that tasks can be completed by the widest possible range of the population, typically the design should accommodate those with dimensions which span the 5th percentile (from

smallest 5% of the female population) female to the 95th percentile (the largest 5% of the male population) male. It is common practice for a Target Audience Description to be produced to inform the design of the workspace, this provides the designer with a set of user characteristics that the design should accommodate.

27. As well as considering the dimensions of a workspace, the design should optimise the layout of the individual components, e.g., different HMIs, within the workspace. The arrangement of HMIs should seek to co-locate equipment and HMIs that are used together to achieve a security function. It should also allow personnel who must work together to be co-located where possible and where this is not possible that adequate communication facilities are provided to support task completion. Where communication between individuals or teams is required the workplace layout should support effective communication between them and should not impinge negatively on others who may be required to perform other tasks at the same time in the same area.

28. Where new workspaces are developed based on existing site practice or on experience from a similar site, the dutyholder should be able to demonstrate that the new workspace will adequately meet the needs of personnel. This may be based on evidence from operational experience and should demonstrate how such information has been used to make changes to the workspace to reflect lessons learned from experience.

29. Inspectors should consider

- Has the dutyholder considered and taken into account the capabilities, characteristics and numbers of the target users who will use the workspaces? Ideally these would be captured in a Target Audience Description or equivalent document which describes the characteristics of the users, particularly where the design of the workspace forms part of large project.
- Has the dutyholder declared and justified appropriate ergonomic standards/references for the design/modification and substantiation of its workspaces?
- Has the dutyholder incorporated appropriate anthropometric and biomechanical (range of movement) considerations and data into its workplace/space and equipment design, dimensions and layout (common practice is to use the 5th percentile female to 95th percentile male range)?
- Has the dutyholder ensured that workers are not cramped or obstructed in any way that would cause distraction of discomfort and encourage hurrying of a task leading to increased potential for human error?
- Has the dutyholder ensured that the workspace dimensions take account of the full range of tasks that need to be undertaken including

maintenance and any requirements for the wearing of protective clothing, carrying of equipment and movement of tooling and components?

- Has the dutyholder demonstrated that the physical arrangement of the workspace has taken account of and is compatible with human perceptual and physical characteristics and limitations, as well as task demands, attributes and characteristics?
- Has the dutyholder employed suitable task analysis methods, e.g., link analysis to determine the relative layout of different HMIs and equipment within individual workspaces?
- Has the dutyholder ensured that workplaces/spaces and the layout of equipment and furniture therein minimise physical and cognitive demands on personnel and the potential for human error caused by disturbances, distractions and disruptions to task performance (e.g., due to movement of people, visitors, location and access/egress routes, briefing rooms, concurrent tasks)?
- Has the dutyholder has conducted a suitable human factors/ergonomics evaluation and testing/trials of the design, development and use of its workplaces/spaces or alternatively can demonstrate suitability and sufficiency of provision using OPEX?

# 8. Environmental Conditions

30. The physical environment can increase both physical and cognitive demand/stress, resulting in distortion or filtering of important sensory information and increased human error potential and/or direct health and safety risks. Dutyholders therefore should demonstrate how environmental conditions in workspaces are controlled paying particular attention to the thermal, visual and auditory environment. Where environmental conditions cannot be controlled e.g., because security important tasks are completed outdoors, dutyholders should demonstrate how environmental impacts on human performance are minimised by the provision of suitable Personal Protective Equipment (PPE) or by staffing arrangements intended to maintain fitness for duty (e.g., fast rotation of staff performing outdoor roles).
This section provides general advice to inspectors regarding good practice expectations for those key environmental factors that impact human performance.

## 8.1. Temperature and Humidity

31. The human response to the thermal environment – temperature and humidity – is affected by factors such as air temperature and velocity, clothing worn and activity levels. Excessive heat or cold can negatively impact mental and physical performance resulting in reduced concentration, vigilance, problem solving, dexterity, sensitivity of touch, increased task completion times as well as perceptual distortion.

32. In indoor environments temperature and humidity can be controlled by Heating, Ventilation and Air Conditioning (HVAC) systems. the required temperature levels should be determined by the amount of physical work required to perform the tasks in the workspace. Where security tasks e.g., searches, pass checks, are conducted outdoors, then appropriate provision should be made to reduce the cognitive and physical stress effects of the thermal conditions. This might include the provision of adequate shelters in which tasks can be undertaken when environmental conditions are challenging or the provision of PPE for short periods where tasks need to be completed in poor environmental conditions. Where PPE is used to reduce the impact of adverse environmental conditions it must be assured that this does not reduce the reliability with which tasks are completed. The dutyholders analysis of the task and selection of PPE should acknowledge that PPE may reduce for example signal detection though auditory or visual signals, dexterity impacting the ability to manipulate tools and equipment and speed of movement.

33. Inspectors should consider

- Is the dutyholder’s HVAC system is capable of sustaining an adjustable range of comfortable air temperatures and desirable relative humidity?

- Has the dutyholder s used appropriate design standards and guidance to derive the most appropriate thermal environment e.g., within security control rooms to support reliable human performance and provided suitable evidence that these standards have been met?
- Has the dutyholder provided as much physical shelter as practicable where operational tasks, maintenance or emergency tasks are required in exposed/outdoor positions?
- Has the dutyholder identified the need for and provided appropriate PPE for tasks that need to be completed in outdoor environment?
- Has the dutyholder has taken into account potential adverse environmental conditions and the impact of PPE when making claims for task feasibility and completion times?

## 8.2. Lighting

34. Appropriate lighting is critical for visual work, including monitoring and detecting tasks, and the maintenance of situational awareness which is a key component of human based security tasks. Essentially when a task relies heavily on vision, the effect of lighting plays a stronger role in task performance. Good lighting makes colours and details easier to discriminate, helps in preventing visual fatigue, and reduces the likelihood of human error.

35. A key point for ensuring operators can use their eyesight to its fullest advantage is to make sure light is distributed to where people will need it most, i.e., at the centre of the visual field. However, it is not ideal to have wide variation in light levels across a room because the eye will need to adapt to the changes in light and will not function effectively until it has achieved this. If a large adaptation needs to occur, this can cause discomfort or glare. Glare can be reduced by not positioning light sources immediately in front of or behind a person, by providing movable or diffusible light sources, by avoiding the use of reflective surfaces and by positioning monitors and Visual Display Units (VDU) at right angles to light sources including natural light.

36. Required illumination levels will differ dependent on the nature of work undertaken. Where detailed or fine discrimination is needed as part of a task then lighting levels will need to be higher. Where a range of tasks is completed in a single workspace then the ability to adjust lighting levels may be beneficial.

37. The colour of lighting is also important, some forms of lighting, e.g., sodium lights, impact on colour perception and can make detailed discrimination of objects more difficult.

38. Where lighting sources may be reduced, e.g., during security events, head or equipment mounted sources of light should be provided if these are necessary to supplement illumination provided by natural or emergency lighting.

39. Inspectors should consider

- Has the dutyholder demonstrated adequate lighting provision for all operational tasks, their demands and foreseeable working conditions, including any tasks required to be performed during emergencies?
- Has the dutyholder considered the impact of degraded lighting on safety and security tasks and provided alternative sources of lighting for such occasions?
- Has adequate provision been made for any requirements for equipment identification, reading textual information, detailed inspection tasks and any fine precision work?
- Is adequate back-up or portable illumination available for maintenance tasks or during emergencies and is there evidence that this equipment is periodically tested?
- Has the dutyholder has used appropriate design standards and guidance to derive the lighting levels required for tasks to support reliable human performance and is suitable evidence provided that these standards have been met?
- Has the impact of factors such as contrast, glare and reflections been identified and appropriately considered in the lighting design?
- Where the dutyholder exploits advanced technologies to display information within control rooms (e.g., large wall-mounted display screens generated by plasma displays, Liquid Crystal Display (LCD) etc) has the legibility and visibility of information displayed by these devices been carefully considered taking into account proposed, or existing, lighting arrangements? Issues of clarity and contrast can seriously degrade the quality of the perceived information.
- Where tasks are completed outside of control rooms in local-to-plant locations, is there evidence that the dutyholder's lighting is adequate to meet the local task requirements?
- Where tasks are completed outdoors has the Dutyholder provided adequate lighting for night time and adverse weather conditions?

## 8.3. Noise

40. Noise in the workplace can be a source of distraction, discomfort and can lead to decrements in human performance and ineffective communication. Exposure to high and/or prolonged levels of noise can also lead to hearing damage. Workplace noise can also have a significant effect on human performance causing an individual to modify their style of task performance which can lead to increased human error potential.

41. The effects of noise on performance are dependent on the degree to which sounds need to be heard to complete a given task. Furthermore, not all noise is bad noise. Overheard speech is almost impossible to 'tune out' but research indicates that work-related conversations are 'good noise' because they can help to keep the team informed about important events (maintaining situation awareness), whereas overheard non-work-related conversations are conversely 'bad noise' because of lack of relevance to the work of the team. Noise has a lesser effect on visual or manual work, although it does usually affect tasks that involve a considerable amount of information processing and decision making.

42. Where tasks are dependent on the detection of auditory signals then background noise levels should not be so high as to mask the signals to be detected. Similarly, where high degrees of communication are required to complete tasks, background noise should not cause misperception of auditory communication nor distract personnel from understanding the content of communications.

43. Inspectors should consider

- Has the dutyholder ensured that the background noise level in control rooms does not impair speech comprehension?
- Is the dutyholder able to demonstrate that all audible alarms and warnings can be heard, or otherwise detected, at all working locations and in all foreseeable conditions?
- Is the dutyholder able to demonstrate that noise levels are controlled in order that security critical communications are not disrupted or masked by background noise. This may include limiting access to security control rooms or providing dedicated spaces where discussions can take place?
- Where there is reliance on Public Address (PA) for communication, its intelligibility is regularly checked in all necessary areas?

# 9. Equipment and User Interfaces

44. A dutyholder's physical protection system and cyber security and information assurance arrangements will require personnel to interact with equipment and the security systems via user interfaces to complete many of the tasks that are necessary for security. A user interface is the means by which a human interacts with a tool, device or system. A user interface typically provides information to a user to alert them that action is required and to determine what action is required. It may provide controls necessary to perform an action e.g., open or close a security door.

45. In order to maximise human performance, it is important that the dutyholder understands the operational requirements and associated task(s) that any piece of equipment or system is used to achieve and ensure that the user needs, operational requirements and performance standards necessary to achieve the task goal are identified. These user needs and operational requirements can then be used to specify the design of the equipment or system user interfaces that need to be developed or procured. Thus, the identification of performance requirements and user needs is a fundamental process for the design or specification of equipment and user interfaces needed to achieve security functions. The identification of operational requirements may come from a task analysis process, review of existing systems and/or learning from experience in relation to use of an extant system. Operational requirements must include the speed with which the system must act, and these should drive the design and form part of the testing of the system both during development and when design is complete.

46. During the design of a set of equipment and user interfaces that meet operational requirements, it is important that relevant ergonomic standards are followed and that end users are involved in testing and confirming the usability of individual features of the user interface using mock-ups and simulations. Having completed the design, trials should be undertaken to demonstrate that the developed system can be operated by end users to achieve reliably the security tasks for which it has been designed. This should include periods of normal operation, heightened threat levels and security event conditions. ONR expects that dutyholders provide evidence of the suitability and sufficiency of all equipment and user interfaces necessary to support tasks important to security as part of the justification that their protective security arrangements can achieve the relevant security outcome and minimise the likelihood of human error.

47. Where dutyholders rely heavily on Commercial Off the Shelf (COTS) rather than bespoke designed equipment, the dutyholder should require suppliers to provide assurance that such equipment and systems meet ergonomic standards and relevant good practice. In addition, the dutyholder should demonstrate awareness of the importance of consistency across the controls and interfaces employed to achieve related tasks. The dutyholder's testing of control interfaces should ensure that presentation of information and

enactment of controls is consistent across all interfaces as far as possible in order to minimise the likelihood of human error. Consistency in design is particularly important where users have to operate at increased levels of stress or in short timescales.

48. In the context of nuclear security, it is likely that the principal equipment and user interfaces required to support tasks important to security will be those used to detect, assess and communicate the appropriate response to security threats. This equipment and associated user interfaces are likely to take the form of surveillance equipment such as CCTV systems and alarms in the form of Intruder Detection Systems (IDS). A key element of tasks required for security will be communication and it is important that the dutyholder fully identifies the communication requirements that support tasks important to security and provides suitable and sufficient equipment that will work in a range of situations e.g., during power outages, to meet these requirements. In many cases, such surveillance and communication equipment will be grouped into one or more security control rooms which bring together information from a number of sources and areas of the site at a single location. The design of such security control rooms or centres, especially when they are being newly developed, should be a topic of interest for security inspectors.

49. Within a user interface, attention should be given to the placement of the various controls, displays and other pieces of equipment that might be used by each individual operator. Controls – such as keyboards, touchscreens, joysticks, trackballs, radio equipment, telephones and switches/levers etc. – should be laid out in order to meet task requirements and be consistent with ergonomic principles. Controls should be appropriately mapped to displays (usually visual displays such as monitors, and other indicators) in order to avoid errors. Displays and controls should also follow cultural conventions (e.g., in the UK the colour red signals danger, the “up” position indicates “off” for switches, a clockwise rotation of dials/ knobs is associated with an increase in an input or output, while horizontal [linear] increments tend to move from left to right, or from bottom to top).

50. For surveillance purposes, good quality cameras and monitors, along with effective placement, will allow personnel to observe the environment well and support their ability to understand the location and likely direction of targets during a dynamic incident – i.e., maintain ‘spatial awareness’. Spatial awareness is an understanding of our location in space and the organisation of objects around us. Camera placement can affect operators’ spatial awareness; if the height of cameras varies considerably it can result in disorientation, especially for more inexperienced operators. One of the key tools allowing CCTV operators to use cameras effectively is the camera map. A good camera map guides operators to select the best camera to view the scene and helps operators to learn camera positions more efficiently. Ideally the numbering of cameras on the map should follow a logical sequence and follow normal conventions (i.e., numbering sequences read from left to right or in clockwise direction). The camera map should represent what the operator

understands about the reality of the environment. labelling of images should allow operators to identify which camera view they are currently looking at in order to maintain situational and spatial awareness.

51. Definitive guidance on the number of screens/images that personnel can reliably monitor is difficult to provide. A number of factors impact on this issue, these include: the type of task undertaken by the CCTV operator (general surveillance v target monitoring), the quality of the image provided by the monitor, whether automation is used to alert operators to the presence of targets, the number of individual stimuli that need to be observed, their density and rate of movement. All of these factors influence the workload inherent in the CCTV monitoring task and drive the number of monitors/screens/images that can be reliably viewed by personnel. Where a dutyholder employs surveillance equipment that requires personnel to monitor a number of screens it should be expected that a justification is made, and evidence provided for the likely reliability of human performance using the system. Detailed Human Factors guidance on CCTV systems and the design of tasks for its use can be found in [8] a CPNI best practice guide on human factors in CCTV control rooms and [9] which provides further detailed guidance on human factors in the design of CCTV systems.

52. Many security control rooms make use of alarms to warn personnel of intruders. Alarms should direct the users' attention to situations requiring timely assessment or action. Alarms should alert, inform and guide required user action. Every alarm should be useful and relevant to the user and have a defined response. Alarms can be differentiated from indications primarily on the basis that they require a response, whereas an indication may only provide information to aid decision making. Alarm levels should be set such that users have sufficient time to carry out the defined response before the situation escalates and minimise the occurrence of false alarms. The alarm system should accommodate the user's capabilities and limitations and be consistent with the principles of alarm design. Control over the setting of alarm levels should be secure in order to reduce the likelihood that the functionality of the alarm system can be reduced or removed by a hostile actor.

53. Alarms are often presented as auditory signals but can also be visually indicated. Auditory alarms must use a frequency that is easily heard against background noise, without employing a loudness which could damage hearing or cause startle effects in control room operators. Visual warnings in contrast should stand out from their background with the use of colour, contrast, etc. The use of sound to convey a warning message can be particularly beneficial in a cluttered visual environment and where particular emphasis needs to be afforded to a serious threat or hazard, as they tend to produce faster reaction times than visual warnings. See [10] for comprehensive guidance on HF issues related to the design and use of alarms.

54. As well as surveillance activities, security personnel may also be required to confirm the identities of personnel and visitors seeking to gain entry to a site or specific area of a site and this is likely to be supported by computer-based

workstations. The design of such workstations and the software systems and user interfaces presenting such information to personnel is likely to be another key area of concern for inspectors. In particular, the clarity with which such systems present information to staff and the potential for confusability of information related to different persons seeking access should be of primary concern.

55. Where dutyholders place reliance on HMI for the achievement of security functions, they should consider ways in which these HMI might fail and if appropriate provide back up or alternative means of supporting the operator's task. Dutyholders should consider how failure of an HMI will be signalled to personnel and ensure that personnel are familiar with the operation of back up equipment. Dutyholders should have protocols in place to inform those who interact with the HMI of its failure and provide authority for making the decision to transfer between HMIs to those who are best placed to make the decision.

56. Inspectors should consider

- Has the dutyholder completed a proportionate level of task analysis to inform the design of equipment and user interfaces required to complete tasks important to security?
- Has the dutyholder employed relevant ergonomics standards to the design of equipment and user interfaces?
- Has the dutyholder provided evidence of end user involvement in the design and usability testing of equipment and user interface important for security?
- Has the dutyholder conducted a proportionate HF / ergonomics evaluation and testing / trials of the design, development and use of equipment and user interfaces and has this demonstrated that the HMI is effective in supporting personnel in all operational states?
- Where testing has identified HF deficiencies in the design, is evidence available to show that these have been addressed and that where appropriate the design has been re-tested and demonstrated as operable?
- Is there a clear documented process that demonstrates how the dutyholder has managed and resolved any conflicts and trade-offs associated with equipment and user interfaces e.g. between security constraints and ergonomics best practice?
- Has the dutyholder carried out an operational experience review to demonstrate that equipment and user interfaces do not result in human failure during the performance of security tasks and during security exercises?

- Has the design and use of equipment and user interfaces been used as input to the development of procedures and operator training needs / competence requirements?
- How the dutyholder has ensured that the design of the equipment and user interfaces provides sufficient and unambiguous information to personnel to maintain situational awareness?
- Has the dutyholder has applied appropriate and consistent coding, labelling, grouping, navigation and layout principles to the design of all relevant user interface controls, communications equipment and displays?
- Do the dutyholder's user interfaces ensure that the presentation of information and placement of controls is appropriate for their purpose, support required response times and minimise the potential for errors?
- Where dutyholders employ CCTV systems as part of their security systems, have they undertaken sufficient analysis to determine factors such as the placement of camera, the number of images, number of screens and demonstrated that decisions in relation to these do not overload operators?
- Does the dutyholder use alarms to alert operators only to situations where responses are required?
- Does the dutyholder's analysis of the alarm system demonstrate that factors such as the number of alarms and the setting of alarm set points, does not overload the operator nor result in a high rate of false alarms?

# 10. Communication Tools

57. A range of communication tools are likely to be required to support tasks important to security. It is likely that primary and secondary forms of communication will be required as these may become disrupted during security events. Types of communication equipment used may include, telephone, radio, PA as well as computer mediated communication such as email or voice and video enabled software. Communication devices and equipment should be tested regularly, and it should be ensured that equipment such as public address is understandable in all areas where it is needed to be heard in a range of environmental conditions.

58. Dutyholders should demonstrate that they have selected the most appropriate communication media for different security tasks and that operation of communication equipment (where this is a secondary task) does not significantly increase workload and disrupt performance on the primary task. Where a range of communication devices are used and these are procured as COTS equipment, dutyholders should ensure that similar communication devices have common interfaces and modes of operation in order to reduce the likelihood that communication will fail or that significant operator attention will be focussed on the operation of the device rather than the communication task being undertaken, increasing the likelihood of communication errors.

59. Communication is important to maintain shared situational awareness. In order to avoid disrupted communication and situational awareness, dutyholders should consider the form and content of messages used to relay information. The use of standard and scripted messages may be employed, particularly where communication might be required in high stress situations. Dutyholders should also demonstrate appropriate use of human performance tools such as pre-job briefs, three-way communication and the phonetic alphabet.

60. Recording aids such as logs etc. should be employed in order that key information to be communicated can be clearly identified and be made available across teams e.g., at shift handovers. These can also facilitate communication between different teams e.g., those in a control room and those on the ground. In modern control room environments, such logs are often held electronically and can be shared across locations. It is important that the language used in such communications and recorded in logs is consistent and employs a formal vocabulary that is shared by all users. Where communication is supported by electronic logs, these can be used to impose structure on recorded information in order that all important issues are communicated when required.

61. Inspectors should consider:

- Has the dutyholder justified and demonstrated the adequacy of the communication tools used for different types of communication, e.g., person to person, person to site, between sites, etc?
- Does the dutyholder design and/or procure communications equipment paying attention to issues such as the consistency of the method of operation, design of the interface and the workload associated with communication tasks?
- Does the dutyholder employ human performance tools to reduce the likelihood of communication errors and ensure all staff are fully trained in their use?
- Does the dutyholder use appropriately designed methods for the recording and communication of information in order to improve shared situational awareness across teams and shifts?

# References

[1] H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003.

[2] ONR, “Security Assessment Principles for the Civil Nuclear Industry,” 2017.

[3] H.M. Government, “Government Functional Standard GovS 007: Security,” [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf.

[4] ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry”.

[5] IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”.

[6] IAEA, “Nuclear Security Series No. 20. Objective and Essential Elements of a State’s Nuclear Security Regime”.

[7] IAEA, “Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011.

[8] Centre for the Protection of Nuclear Infrastructure, “Human Factors in CCTV Control Rooms: A Best Practice Guide”.

[9] R. Pikaar, Human Factors Guidelines for the design of CCTV Systems., 2015.

[10] EEMUA, Alarm Systems: A Guide to Design, Management and Procurement. EEMUA Publication 191. 3rd Edition, 2013.

# Glossary and Abbreviations

| | |
|---|---|
| AID | Automatic Intruder Detection |
| COTS | Commercial Off the Shelf |
| CPPNM | Convention on the Physical Protection of Nuclear Material |
| CS&IA | Cyber Security and Information Assurance |
| FSyP | Fundamental Security Principle |
| HMI | Human Machine Interface |
| HVAC | Heating Ventilation and Air Conditioning |
| IAEA | International Atomic Energy Agency |
| LCD | Liquid Crystal Display |
| NISR | Nuclear Industries Security Regulations |
| NM | Nuclear Material |
| NSS | Nuclear Security Series |
| ONR | Office for Nuclear Regulation |
| ORM | Other Radioactive Material |
| PA | Public Address |
| PPE | Personal Protective Equipment |
| PPS | Physical Protection System |
| SNI | Sensitive Nuclear Information |
| SPF | Security Policy Framework |
| SyAP | Security Assessment Principle |
| SyDP | Security Delivery Principle |
| TAG | Technical Assessment Guide |