|  |
| --- |
| **Early Initiation of Safety Systems** |
| **Doc. Type** | ONR Technical Assessment Guide (TAG) |
| **Unique Doc. ID:**  | NS-TAST-GD-010  | **Issue No.:** | 7.1 |
| **Record Reference:** | 2021/0057204 |
| **Date Issued:** | Dec-2022 | **Next Major Review Date:** | Dec-2024 |
| **Prepared by:** |  | ONR Inspector  |
| **Approved by:** |  | Deputy Professional Lead – Human and Organisational Capability |
| **Professional Lead:** |  | Professional Lead – Human and Organisational Capability |
| **Revision Commentary:** | This is a major update to improve clarity of this TAG.Issue 7.1 - Minor update to remove extant URLs from the document to mitigate potential configuration control issues arising because of changes to third-party web domains. |

**Table of Contents**

[1. Introduction 3](#_Toc121119726)

[2. Purpose and Scope 4](#_Toc121119727)

[3. Relationship to Licence and other Relevant Legislation 5](#_Toc121119728)

[4. Relationship to SAPs, WENRA Reference Levels and IAEA Safety Standards Addressed Legislation 7](#_Toc121119729)

[4.1. SAPs and Interfacing TAGs 7](#_Toc121119730)

[4.2. WENRA Guidance 9](#_Toc121119731)

[4.3. IAEA Guidance 9](#_Toc121119732)

[5. Advice to Inspectors 12](#_Toc121119733)

[5.1. Provision of suitably sized safety systems and appropriate allocation of safety systems to operators 12](#_Toc121119734)

[5.2. Assessment of claimed actions 13](#_Toc121119735)

[5.3. Determining the time required for manual actions 14](#_Toc121119736)

[5.4. Early operator action within the 30-minute period 15](#_Toc121119737)

[5.5. Deviation from the 30-minute design assumption 16](#_Toc121119738)

[5.6. Time requirements for local to plant actions 17](#_Toc121119739)

[References 20](#_Toc121119740)

[Glossary and Abbreviations 21](#_Toc121119741)

[Appendix 1 - Definition of the 30-minute Period 22](#_Toc121119742)

# Introduction

1. ONR has established its Safety Assessment Principles (SAPs) [1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other 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 (TAG) is one of these guides.

# Purpose and Scope

1. This TAG contains guidance to advise and inform ONR staff in the exercise of their regulatory judgment in relation to the interpretation of Safety Assessment Principles (SAPs) ESS.8 ‘Automatic initiation’ and ESS.9 ‘Time for human intervention’ and their underpinning paragraphs 404 and 405. These provide advice to inspectors on the design of safety systems and recognise the link to related Human Factors SAPs when such systems are manually initiated.
2. The guidance is intended to ensure that engineered safety systems are designed to keep the facility within its safe operating limits without the need to claim operator action to initiate, moderate or disable safety system action within approximately 30 minutes of the indicated start of the requirement for protective action. The guidance also considers those operator actions that may be performed within the 30-minute period and sets out ONR’s expectations about the nature of, and support for, such actions.
3. The guidance presented here should be applied in association with Technical Assessment Guidance which states ONR’s expectations concerning the treatment of HF throughout the facility life cycle [2] and related underpinning guidance on HF approaches and methodologies. Reference should also be made to NS-TAST-GD-003 [3] which offers guidance on the application of SAPs concerned with engineered safety systems, including protection and actuation systems.
4. This document provides advice to inspectors on the following elements.
* Provision of suitably sized safety systems and appropriate allocation of safety functions to operators
* Assessment of claimed actions
* Determining the required time for manual actions
* Early operator action within the 30-minute period
* Deviation from the 30-minute design assumption
* Time requirements for local actions

# Relationship to Licence and other Relevant Legislation

1. The Licence Conditions (LC) [4] place legal requirements on the licensee to make and implement arrangements to ensure that safety is being managed adequately. The Licence Conditions provide a legal framework which can be drawn on in assessment. LC 27 is of particular relevance in that it requires suitable and sufficient safety systems to be provided.
* Licence Condition 27: Safety Mechanisms, Devices and Circuits -
the licensee shall ensure that a plant is not operated, inspected, maintained or tested unless suitable and sufficient safety mechanisms, devices and circuits are properly connected and in good working order.
1. ESS 8 and 9 provide advice to inspectors as to what is a suitable safety system in the case where they need to be initiated early.
2. If a safety system is not automatic but manually initiated the LCs require that staff are suitably trained and supported by suitable procedures and other arrangements (LC 10,11,12, 23, 24 and 26).
* Licence Condition 10: Training - the licensee shall make and implement adequate arrangements for suitable training for all those on site who have responsibility for any operations which may affect safety.
* Licence Condition 11: Emergency Arrangements - without prejudice to any other requirements of the conditions attached to this licence the licensee shall make and implement adequate arrangements for dealing with any accident or emergency arising on the site and their effects.
* Licence Condition 12: Duly authorised and other suitably qualified and experienced persons - the licensee shall make and implement adequate arrangements to ensure that only suitably qualified and experienced persons perform any duties which may affect the safety of operations on the site, or any other duties assigned by or under these conditions or any arrangements required under these conditions.
* Licence Condition 23: Operating Rules - the licensee shall, in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation and to identify the conditions and limits necessary in the interests of safety.
Such conditions and limits shall hereinafter be referred to as operating rules.
* Licence Condition 24: Operating Instructions - the licensee shall ensure that all operations which may affect safety are carried out in accordance with written instructions hereinafter referred to as operating instructions.
* Licence Condition 26: Control and Supervision of Operations - the licensee shall ensure that no operations are carried out which may affect safety except under the control and supervision of suitably qualified and experienced persons appointed for that purpose by the licensee.

# Relationship to SAPs, WENRA Reference Levels and IAEA Safety Standards Addressed Legislation

## SAPs and Interfacing TAGs

1. The key SAPs for this guidance are ESS.8 and 9.
* SAP ESS.8: “For all fast-acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).”
* SAPs supporting paragraph 404: “The design should be such that the operators or other facility personnel cannot negate a correct safety system action but can initiate safety system functions and perform the necessary actions to deal with circumstances that might prejudice safety. See also EHF principles, and in particular Principles EHF.1 to EHF.5.”
1. ESS.8 requires that safety systems should be initiated automatically for fast acting faults. Further guidance is provided on allocation of function between engineered systems and humans in NS-TAST-GD-064 [5]. SAPs supporting paragraph 404 requires that when a safety system is started automatically the operators cannot terminate it however it allows for operators to initiate safety systems functions or take other actions necessary to maintain safety. This is discussed further in section 5.3.
2. ESS 9 discusses cases where human action is required.
* SAP ESS.9: “Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales over which the safety system will need to operate unaided should be demonstrated to be sufficient.”
* SAPs supporting paragraph 405: “In keeping with internationally accepted relevant good practice for power reactors, no human intervention should be necessary for approximately 30 minutes from the start of the safety system initiation.”
1. ESS.9 requires that the licensee demonstrates via analysis that a safety system claimed in response to a fast-acting fault provides sufficient capacity such that operator actions are not required for a period of time following the demand for the system. Where operator actions are then required to achieve safety, analysis should demonstrate there is sufficient time for operators to detect, diagnose, plan and complete the actions required. SAPs supporting paragraph 405 states that at least 30 minutes should be available before human action is required. Demonstration of this requires suitable and sufficient modelling and substantiation of claims on both the engineering systems and the tasks required to initiate them. This is to provide the necessary confidence that they will operate as intended. All of the Engineering Human Factor (EHF) principles are relevant to this to some degree. However, EHF.2, 5, 10 are particularly relevant and EHF. 6, 7, 8, 9, 11, 12 support demonstration that a sufficient level of human reliability is achieved as required by EHF.10.
* SAP EHF.2 “When designing systems, dependence on human action to maintain and recover a stable, safe state should be minimised. The allocation of safety actions between humans and engineered structures, systems or components should be substantiated.”
* SAPs supporting paragraph 446 “Where administrative safety measures are identified to deliver safety functions (see Principle EKP.5) the guidance in paragraphs 155 and 156 should be followed. Principles ESS.8 and ESS.9 on safety system initiation are also relevant here.”
1. EHF.2 is clear that in general automatic safety system operation is preferred over manual operation following the hierarchy of control described in paragraph 155 of the SAPs. Substantiation of the allocation to an operator requires that the licensee demonstrates that the allocated action is feasible and sufficiently reliable. This can be achieved following EHF. 5 and 10 respectively.
* EHF.5 “Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute.”
* EHF.10 “Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety.”
1. Safety measures should be automatic rather than manual when possible (EKP.5, para 155 and EHF.2). This is particularly so for fast acting faults (ESS.8). Where safety systems are initiated by the operator the licensee must demonstrate the time is sufficient (ESS. 9). For any safety action the licensee must demonstrate that the action is feasible and sufficiently reliable (EHF.5 and 10) and that factors that support human actions have been optimised (EHF. 6, 7, 8, 9 and 11).
2. The following TAGs are also relevant:
* NS-TAST-GD-003 - Safety Systems [3]
* NS-TAST-GD-006 - Design Basis Analysis [6]
* NS-TAST-GD-063 - Human Reliability Analysis [7]
* NS-TAST-GD-064 - Allocation of function between human and engineered systems [5]
1. Assessment of safety actions allocated to operators is discussed further in section 5.7.

## WENRA Guidance

1. ONR considers that the Western European Nuclear Regulator’s Association (WENRA) Reference Levels are Relevant Good Practice (RGP) as defined in NS-TAST-GD-005 [8]. The WENRA Reactor Safety reference levels for existing reactors [9] section 9.3 states that:
* “Activations and manoeuvring of the safety functions shall be automated or accomplished by passive means such that operator action to initiate safety systems is not necessary within 30 minutes after the initiating event. Any operator actions required by the design within 30 minutes after the initiating event shall be justified.”
* “The control room staff have to be given sufficient time to understand the situation and take the correct actions. Operator actions required by the design within 30 minutes after the initiating event have to be justified and supported by clear, documented procedures that are regularly exercised in a full scope simulator.”
1. This is consistent with the SAPs with the following two exceptions.
* That WENRA guidance is limited to reactors whereas the SAPs do not limit the requirement specifically to reactors.
* That WENRA guidance takes the time as starting from the initiating event and the SAPs take it from the time the operator is made aware.

## IAEA Guidance

1. The International Atomic Energy Agency (IAEA) Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2014 and are recognised by ONR as RGP.
2. Relevant IAEA guidance can be found in SSR-2/1 [10] which states the following.
* “The design: ………(d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized”.
* “5.11 Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions.
* 5.12 Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems or on other operator actions. For such cases, the time interval between detection of the abnormal event or accident and the required action shall be sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process.
* 5.13 The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.”
1. This aligns with the SAPs described in section 4.1 to 4.7. SSG-2 [11].
* 7.37. For conservative safety analysis, credit should not be taken for operator diagnosis of the event and for initiating the necessary actions until after a conservatively specified time. The timing assumed in an analysis should be justified and validated for the specific reactor design; for example, the minimum specified time may be 30 minutes for control room actions or 60 minutes for field actions.
* 7.38. Correct actions of plant staff to prevent an accident or mitigate its consequences should only be taken into account in the analysis if it can be shown that the event sequence and the plant specific boundary conditions allow for carrying out the assumed actions. The conditions to be considered include the overall context in which the event sequence takes place, the working environment in the control places, written procedures, and the relevant staff’s training status and access to necessary information.”
1. SSG-2 aligns with ESS.8 as it requires a minimum time of 30 minutes for control room staff to operate a safety system. It also requires a demonstration that there is sufficient time which aligns to ESS.9.
2. It should be noted that SSG-2 provides graded expectations for different types of deterministic safety analysis. Consistent with ONR’s expectations, the text above applies only for design basis accidents. SSG-2 proposes best-estimate assumptions for deterministic analysis substantiating claims made for normal operation and design extension conditions (for example severe accidents)”.

# Advice to Inspectors

1. The design of safety systems and the substantiation of their safety function are intrinsically linked. Very early in system design it is appropriate to use conservative design assumptions supported by experience of operation of similar systems as a starting point where these are available. As the design matures assumptions need to be tested and validated. This may result in design changes if the early assumptions prove not to be sufficiently conservative. The guidance here is therefore presented both to guide assessment of plant design and validation of claims on systems, in particular assessing claims on the operator to operate safety systems.
2. The following advice to inspectors is provided to describe how claims on manual early initiation of safety systems should be assessed. This is presented in the following sections.
* Provision of suitably sized safety systems and appropriate allocation of safety functions to operators
* Assessment of claimed actions
* Determining the required time for manual actions
* Early operator action within the 30-minute period
* Deviation from the 30-minute design assumption
* Time requirements for local to plant actions

## Provision of suitably sized safety systems and appropriate allocation of safety systems to operators

1. Safety systems are provided to reduce the frequency, or limit the consequences, of fault sequences, and to achieve and maintain a defined stable safe state (SAP ESS.1). Automatic safety system initiation is normally regarded as being a more reliable means of instigating the correct functioning of appropriate plant and equipment than human (“operator”) action (EKP.5), especially where early protective action is required. Licensees should therefore be able to demonstrate that early protection against design basis faults is achieved through automatic initiation of adequately sized safety systems (for example sufficient volume of cooling water that no manual initiation is required early in the scenario) and that the safety case does not need to claim early action by operators to initiate, moderate or disable safety systems. Allocation of function is subject to application of the overriding ALARP principle.
2. Further guidance on allocation of function between automatic and manual systems is provided in in NS-TAST-GD-064 ‘Allocation of function between human and engineered systems’ [15].
3. The SAPs (ESS.8) set an expectation that safety systems should not require operator action for a minimum of 30 minutes and no human intervention should then be necessary to deliver the safety function(s). The extent to which this is achieved in practice or whether it is reasonably practicable to do more should be informed by the significance of the safety system (and associated operator action) to successfully delivering the necessary safety functions identified in safety case. Inspectors should confirm that where safety functions are required within short timescales these are allocated to engineered systems with automatic initiation. The licensee’s analysis should demonstrate that the systems have the capability and capacity to provide the safety function without the need for operator interaction for a minimum period of 30 minutes and that sufficient time is available for the operator to act (see below).

## Assessment of claimed actions

1. All human actions and controls required for safety should be identified (SAP EHF.3) and subject to proportionate task analysis (SAP EHF.5) including those claimed in short timescales. This may be undertaken later in the design process than the initial sizing of automatically initiated engineered safety systems. The analysis should however be undertaken early enough to inform the development of the design such that any necessary changes to support timely operator action can be implemented. Human Reliability Analysis (HRA) should be conducted as part of Design Basis Analysis (DBA), Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA) aspects of the safety case (SAP EHF.10).
2. Guidance on the factors to be considered when substantiating claims on operators is presented in the following guidance.
* NS-TAST-GD-063 - Human Reliability Analysis [7]
* NS-TAST-GD-027 - Training and Assuring Personnel Competence [12]
* NS-TAST-GD-059 - Human Machine Interface [13]
* NS-TAST-GD-060 - Procedure Design and Administrative Controls [14]
* NS-TAST-GD-061 - Staffing Levels and task organisation [15]
* NS-TAST-GD-062 - Workplaces and Work Environment [16]

## Determining the time required for manual actions

1. When safety systems are operated by humans, sufficient time must be allowed (ESS.9). The time available and time required for operator action are key factors to demonstrate that a claimed action is feasible and reliable. The time available for operator action should be determined by engineering modelling of the fault and system response. The required time for operator action can be determined by task analysis (EHF.5), simulation and / or observation. For all operator tasks claimed in the DBA, PSA or SAA it is necessary to show that there is sufficient time available to support effective task performance (EHF.10).

### Design Basis Analysis

1. Paragraph 405 of the SAPs states “no human intervention should be necessary for approximately 30 minutes from the start of the safety system initiation.” The definition of this 30-minute period is described in detail in Appendix 1.
2. The requirement for a 30-minute period before human intervention is necessary is identified in IAEA and WENRA documents (section 3) that relate to power reactor main control room actions. It is recognised that power reactors are complex, subject to a range of faults where diagnosis may not be straightforward, and therefore that it is particularly important to allow sufficient time for such diagnosis. Licensees of other types of facility where systems are less complex or where the range of faults is limited, may consider the application of the 30-minute period to have limited value. Where this is the case, the licensee should justify with clear supporting arguments why the 30-minute design assumption should not be applied.

### Probabilistic Safety Analysis

1. Analysis that supports the PSA should be made on a best estimate basis (SAPs paragraph 655) and supporting analysis should consider NS-TAST-GD-063 [7]. There is therefore no requirement to assume 30 minutes for detection, diagnosis and planning prior to the action. The timing of an action claimed in the PSA should be assessed on a best estimate basis.

### Severe Accident Analysis

1. Rigorous application of DBA should ensure that severe accidents are highly unlikely, however suitable and sufficient severe accident analysis is still required to ensure that risks are reduced So Far As Is Reasonably Practicable (SFAIRP), and to support the facility PSA. SAPs ESS8, ESS9 and underpinning paragraphs 404 and 405 apply specifically to design basis fault sequences and ONR’s expectations concerning claims for operator safety action within the 30-minute period do not apply to claims for early operator action to mitigate severe accidents, as referred to in SAPs FA.15 and FA.16. Claims made on the operator should be scrutinised as appropriate to their importance in line with the general guidance on claims for operator action in NS-TAST-GD-063 [7].
2. Although it is appropriate to take a best estimate approach to analysing severe accident fault sequences (SAPs paragraph 505) the licensee’s assessments of claims for operator action should take due account of the factors that may impact upon human performance in such sequences. The operator's direct experience of beyond design basis events will have been restricted to emergency exercises and, perhaps, some sessions with the limited models in training simulators. These limitations, together with the potential stress and uncertainty associated with severe accidents, make it important to treat any claims for early operator action in response to such events with considerable caution.
3. If the safety case is unable to substantiate the claims that are made on operator performance, then the facility design, or its mode of operation, should be modified to remove the need to claim operator action or to modify that claim such that it can be substantiated.

## Early operator action within the 30-minute period

1. SAPs ESS.8, ESS.9 and underpinning paragraphs 404 and 405 are intended to minimise the potential for inappropriate operator action in the early stages of a disturbance. However, for some faults, early operator action could also have a positive impact on safety by reinforcing the safety system.
The licensee may also wish to initiate early operator action for commercial reasons, where this is the case licensees should demonstrate that these actions do not have the potential to negate the actions of a correctly functioning safety system.
2. The plant design should be such that the operators or other facility personnel cannot negate a correct safety system action but can initiate safety system functions and perform the necessary actions to deal with circumstances that might prejudice safety (paragraph 404). However, no human intervention should be necessary for approximately 30 minutes from the start of the safety system initiation (para 405). The following principles may therefore be applied.
* Since an operator may determine a need for a safety system function before it is initiated automatically, then manual initiation should be possible provided that this does not negate or impair correct safety system action overall.
* If a safety system fails to operate correctly, or to achieve its desired functional performance when a demand is placed upon it by a protection signal, the operator should not be prevented from carrying out actions during the 30-minute period in order to restore the correct functioning of that system or to achieve an effective transition to a safe state. This is consistent with WENRA guidance (para E10.9 [6]) which states “…the reactor protection system shall not prevent operators from taking correct actions if necessary in design basis accidents”.
* Where operator action is claimed to reinforce or support safety system performance within the 30-minute period, it is particularly important that there should be a clear and direct means of confirming to operating personnel that a demand for safety system action has arisen, and if so whether the safety system has operated correctly, and whether any limiting condition has been exceeded which takes the safety system beyond its substantiated capability (SAP ESS.13). The safety case should demonstrate that Human Factors principles have been applied in the design of facility, equipment and administrative arrangements and that reliable operator performance is supported (SAPs EHF.4, EHF.6 and EHF.7 and paras 446, 456).
* During the 30-minute period it should not be possible for operators to disable or moderate a functioning safety system so long as a protection signal continues to demand the operation of that system (in other words the safety system is responding correctly given a current demand). (ESS.9 and para 404).

## Deviation from the 30-minute design assumption

1. SAPs ESS.8, ESS.9 and underpinning paras 404 and 405 should be regarded as general principles against which a facility design is assessed. There should be a strong expectation that they represent relevant good practice and for a new facility at the design stage are met SFAIRP. For existing facilities, if safety cases do not comply with this principle, claims for operator action to initiate, support or moderate safety system operation should be assessed on a case-by-case basis. In such circumstances, licensees should provide a robust ALARP argument and justification of the claim for early operator action. This should demonstrate why it is not reasonably practicable to achieve the desired safety system performance automatically. This should include Human Factors analysis to describe the claimed operator actions, establish their feasibility and identify potential improvements. Justification that there is sufficient time should be robust and should consider ongoing tasks, parallel tasks, time for detection, diagnosis, and planning, the analysis should also show there is a margin in the timescales for operator action to account for uncertainty in response and modelling.
2. Guidance on the factors to be considered when substantiating claims on operators is presented in NS-TAST-GD-063 [7] but some of the key expectations for short duration claims are drawn out below.
* Suitable and sufficient alarms and other indications of the need for operator action should be available within the control room. These should be unambiguous, obvious and robust. They should be sufficiently salient and of sufficient priority to be detected in the available time. Inspectors need to be satisfied that the potential for the operator failing to detect the relevant alarms and indications, and identify the correct actions, is minimised.
* The actions required of the operator should be simple, well-understood and must be stated clearly in operating instructions.
* Feedback should be provided to confirm the effectiveness of the operator's actions. Inspectors need to be satisfied that the potential for error in carrying out the actions is understood and minimised.
* The licensee should confirm a commitment to carry out regular training which covers the operator's tasks, and monitoring of performance. Emphasis should be placed on the decision-making aspects of the tasks, noting the pressures which may be brought about by the potential safety significance of the actions, coupled with their lack of frequency and potential commercial impact.
1. Further guidance on the factors to be considered when reviewing such claims is provided in separate TAGs.
* NS-TAST-GD-027 [12]
* NS-TAST-GD-059 [13]
* NS-TAST-GD-060 [14]
* NS-TAST-GD-061 [15]
* NS-TAST-GD-062 [16]

## Time requirements for local to plant actions

1. IAEA SSG2 [11] extends the 30-minute rule and includes provision for allowing 60-minutes for field (local to plant) actions. The SAPs do not include such a 60-minute design assumption but the requirements for task substantiation include local actions if they are required for safety system initiation. This assessment should include consideration of whether there is adequate time available to perform the local action.
2. Application of a 60-minute design assumption may be appropriate early in a design process but will need to be substantiated and may not be sufficient even on a best estimate basis. Substantiation of local actions needs to consider if the action is directed from the main control or the need for it is determined locally. These are discussed below.

### Actions directed from the Main Control Room

1. Calculation of when a local action can be credited with completion should consider the whole sequence of events from initial indication of the safety system demand (the fault), through detection, diagnosis, communication, travel and action. For the DBA a minimum of 30 minutes should be allowed for the detection/diagnosis phase in the main control room before modelling the remaining parts of the task.

### Independent local actions

1. The ESS.8 and ESS.9 are intended to ensure that operators managing unexpected events have time to overcome initial stress, make sense of a potentially large number of indicators and consider their response carefully. The same may be true for field operators making a diagnosis and the
30-minute design assumption should therefore generally be followed for local fault diagnosis.
2. However, licensees may wish to argue that application of the 30-minute design assumption is overly conservative in some circumstances such as when:
* the operator is directly involved in the task,
* the operator is provided with a clear and unambiguous signal that a fault is initiated,
* there is limited or no decision making required,
* there are no conflicting demands,
* the required action is simple,
* the operator has all necessary information and equipment immediately available and,
* there is clear feedback that the action has been successful.
1. For example, a crane driver might be credited with maintaining control of a load or reacting to an alarm in a time less than 30 minutes as the driver is engaged with the task (in control), safety can be achieved simply by stopping the crane, the number of faults is limited, those faults are clear to the driver and the action is always the same, to stop.
2. On other nuclear plant such as chemical plants, the protection against the
on-site consequences of design basis faults may in many cases be to evacuate or to make safe and evacuate. In such cases the time claimed for evacuation needs to be supported by appropriate analysis and may be less than 30 minutes.
3. Inspectors should consider whether claimed field operator tasks have been adequately substantiated using the guidance in NS-TAST-GD-063 [7] whether or not the 30-minute rule has been met. This must take into account the particular environmental conditions that may arise as a result of the fault / hazard or because of the location of the required action.

# References

|  |  |
| --- | --- |
| [1]  | ONR, “Safety Assessment Principles (SAPs) (2019/367414)”. |
| [2]  | ONR, “NS-TAST-GD-058 - Human Factors Integration (2020/127021)”. |
| [3]  | ONR, “NS-TAST-GD-003 - Safety Systems (2020/260295)”. |
| [4]  | ONR, “Licence Condition Handbook (February 2017)”. |
| [5]  | ONR, “NS-TAST-GD-064 - Allocation of Function Between Human and Engineering Systems (2020/265795)”. |
| [6]  | ONR, “NS-TAST-GD-006 - Design Basis Analysis (2020/37019)”. |
| [7]  | ONR, “NS-TAST-GD-063 - Human Reliability Analysis (2020/265784)”. |
| [8]  | ONR, “NS-TAST-GD-005 - Guidance on the Demonstration of ALARP (2020/230789)”. |
| [9]  | WENRA, “WENRA Safety Reference Levels for Existing Reactors (Revision 2020),” [Online].  |
| [10]  | IAEA, “IAEA Safety Standards - Safety of Nuclear Power Plants: Design (SSR 2/1 Rev.1),” [Online]. Available: <https://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf.> |
| [11]  | IAEA, “IAEA Safety Standards - Deterministic Safety Analysis for Nuclear Power Plants (SSG-2, Rev.1),” [Online]. Available: <https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1851_web.pdf>. |
| [12]  | ONR, “NS-TAST-GD-027 - Training and Assuring Personnel Competence (2017/278941)”. |
| [13]  | ONR, “NS-TAST-GD-059 - Human Machine Interface (2020/265758)”. |
| [14]  | ONR, “NS-TAST-GD-060 - Procedure Design and Administrative Controls (2020/265773)”. |
| [15]  | ONR, “NS-TAST-GD-061 - Staffing Levels and task organisation (2020/127012)”. |
| [16]  | ONR, “NS-TAST-GD-062 - Workplaces and Work Environment (2020/297470)”. |

# Glossary and Abbreviations

ALARP As low as reasonably practicable

DBA Design Basis Analysis

HF Human Factors

HRA Human Reliability Analysis

HSE Health and Safety Executive

IAEA International Atomic Energy Agency

PSA Probabilistic Safety Assessment

ONR Office for Nuclear Regulation

RGP Relevant Good Practice

SAA Severe Accident Analysis

SAP Safety Assessment Principle(s)

SFAIRP So Far As Is Reasonably Practical

TAG Technical Assessment Guide(s)

WENRA Western European Nuclear Regulators’ Association

# Appendix 1 - Definition of the 30-minute Period

1. SAPS paragraph 405, in support of SAP ESS.9, states ONR’s expectations that there should be a nominal period of approximately 30 minutes, commencing from the start of the safety system initiation, within which the safety of the facility should not be dependent upon the operator carrying out any control actions which actuate, or contribute towards the control, or effectiveness, of safety systems.
2. The 30-minute period stated in SAP’s paragraph 405 is not based on a systematic analysis of the time which the operator needs to prepare a response to design basis events. Any time estimate arising from such an analysis would be event-specific and would depend upon the design of the facility, how it is operated and how operator actions are supported. Rather, paragraph 405 is a deterministic design principle intended to ensure suitably sized engineered safety systems are provided which reduce the reliance on operator action in short timescales. This is to reduce the potential for erroneous operator action to impact on safety. This principle is based on the premise that the likelihood of operator error is highest immediately after the onset of an event when the operator may be exposed to a stressful situation and presented with a large number of indications and alarms at a time when he/she is not fully aware of the situation. The principle therefore acknowledges that the risk of error falls as the operator has more time to reach an informed and considered decision.
3. SAP ESS.13 requires that there should be a direct means of indicating to the operator that a demand for safety system action has arisen. For the purposes of modelling the operators’ response, the point at which the 30-minute period is taken to commence should correspond not to the requirement for safety system actuation, but to the moment when the demand for safety system operation is indicated to the operator (although for many events the initiating event and the indication are likely to occur at much the same time). A full 30-minute period should be available for the operator to detect the problem, monitor the developing situation, make a diagnosis and plan a response, before it may become necessary to claim operator safety action. This interpretation allows the schedule presented in Figure 1 to be determined for those design basis fault sequences which claim operator safety actions:



Figure 1: Key stages arising from application of SAP ESS.8 and paragraph 405 to design basis events

**Key**:

**T0** - Demand for safety system operation.

**T1** - Indication of demand for safety system operation to operator.

**Tp**- The time when it is estimated that the event has been detected, the problem diagnosed, and the operators are ready to act.

**T2** - The point from which manual safety system actions may ordinarily be claimed.

**Tc** - The point when it is estimated that operators will have carried out the required action.

**T3** - The last time by which safety system operation must have commenced for facility to be brought to safe (e.g., shutdown) condition.

**T4** - Facility in safe quiescent state.

1. Figure 1 shows a safety event. The period between T0 and T1 is the time for the system to detect the fault and to alert the operator. The time between T3 and T4 is the time required for the system to operate to address the fault once initiated by the operator. Time between T1 and T3 is available for the operator to detect, diagnose, plan and act.
2. The safety case should define the following.
* The time for the system to detect and alert the operator, T0 to T1.
* The time by which the system should be initiated T3.
1. These are times for the engineered systems and need to account for dynamic nature of the event and the engineered systems required to detect, measure and provide information to the operators. These times are key parts of the fault analysis and must be available as part of the safety case. They can be calculated, estimated or measured but should be suitably conservative to allow for uncertainty.
2. The first phase of the operator response (T1 to Tp) is the time required for the operator to detect, diagnose and plan actions. This time should be estimated on a conservative basis and take into account the effect on the operator of a sudden onset condition.
3. The second phase of the operator response (T2 to Tc) is the time for the operator to carry out the required actions. This should be claimed to start at T2. This should be no earlier than 30 minutes unless Tp is greater than 30 minutes in which case T2 is the same as Tp. For the mission to be successful it must be shown that Tc occurs before T3.
4. The quality of the human factors modelling used to underpin the timings is important and should incorporate some initial time for orientation where the operator seeks to complete any ongoing task, make sense of the situation, and deal with the potentially high number of alarms and indications. It should also take account of the degree of confidence which exists in relation to the fault progression with any uncertainties understood and reflected in the modelling. It is good practice [8] to carry out sensitivity analysis to understand whether any foreseeable delays to timings could result in cliff edge effects.Any time between Tp and T2 is a margin and is an indication as to whether the 30-minute rule is adding conservatism. The inspector should consider whether the licensee has demonstrated that the margin is sufficient to account for the uncertainty of modelling given the evidence presented.
5. The inspector should bear in mind that available time itself is never the sole, and may not be the dominant, influence on operator performance. Other pertinent factors include; the task demands, interface design, provision and clarity of procedures, adequacy of training, working environment etc. The inspector should ensure that claims on operator safety action are adequately supported as discussed in section 5.5.
6. The 30-minute rule aims to give operators time to process unexpected events. It is applicable therefore to the initial parts of a scenario where the operator has to detect, diagnose and engage with an event. As the scenario progresses and new information is presented, the 30-minute rule does not require that the clock is restarted, and a new 30-minute period applied. The licensee would still need to show there is sufficient time to carry out subsequent tasks reliably but there is no requirement to re-apply the
30-minute rule.