ONR GUIDE			
Early Initiation of Safety Systems			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-010 Revision 5		
Date Issued:	November 2017	**Review Date:**	November 2020
Approved by:	E Vinton	Professional Lead	
Record Reference:	TRIM Folder 1.1.3.776. (2017/435162)		
Revision commentary:	Revision		

TABLE OF CONTENTS

Published 11/17

1. INTRODUCTION

1.1 ONR has established its Safety Assessment Principles (SAPs) which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide is one of these guides.

2. PURPOSE AND SCOPE

2.1 This TAG discusses how SAPs ESS.8 and ESS.9, and their underpinning paragraphs 404 and 405, should be interpreted. Reference is also made to related Human Factors (HF) SAPs EHF.5 and EHF.8 and paragraphs 446 and 456. 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.

2.2 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.

2.3 On nuclear chemical plants, the protection in many cases against the on-site consequences of design basis faults is to evacuate. This is itself a safety measure, and lies outside the scope of this TAG, which addresses cases where safety systems need to be activated by personnel. The time claimed for evacuation needs to be supported by appropriate analysis, and may be less than 30 minutes.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 The Nuclear Site Licence Conditions [4] place legal requirements on the licensee to make and implement arrangements to demonstrate that safety is being managed adequately. The following Licence Conditions are pertinent to the application of SAPs ESS.8 and ESS.9 and underpinning paragraphs 404 and 405. They will be considered when assessing claims for operator action made in a licensee's safety case.

> **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 andexperienced 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 14: Safety Documentation - without prejudice to any other requirements of the conditions attached to this licence the licensee shall make and implement adequate arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation.

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.

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.

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

4.1 This TAG is intended to interpret three distinct elements relating to the early initiation of safety systems. These are the automatic initiation of safety systems (discussed in Section 4.1); the practice for limiting claims made for operator safety actions within approximately 30 minutes (discussed in Section 4.2); and the scope for allowing operator action which may enhance, but does not impede, the operation of safety systems (discussed in Section 4.3). Some general considerations are summarised in Section 4.4. SAPs relevant to this guidance include the following:

SAP ESS.8 states:

“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).”

Supporting paragraph 404 states:

“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.”

SAP ESS.9 states:

“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.”

Supporting paragraph 405 states:

"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."

SAP EHF.2 states:

"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."

Supporting paragraph 446 states:

"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."

SAP EHF.7 states:

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

Supporting paragraph 456 states:

"The user interface should:

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

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

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

(d) support effective diagnosis of plant deviations;

(e) enable the operator to determine and execute appropriate actions including those needed to overcome failures of automated safety systems or to reset a safety system after its operation; and

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

4.2 ONR considers that the Western European Nuclear Regulator's Association (WENRA) Reference Levels are Relevant Good Practice (RGP) as defined in TAG NS-TAST-GD-005 "ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)" [5]. The guidance presented here is consistent with WENRA Reactor Safety reference levels Issue E Design Basis Envelope for Existing Reactors [6]. S 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."

4.3 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.

4.4 The guidance in this TAG is also consistent with IAEA guidance:

SSR-2/1 (Rev 1): Safety of Nuclear Power Plants: Design [7] states:

> "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"
>
> "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.
>
> 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.
>
> 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."

5. ADVICE TO INSPECTORS

5.1 AUTOMATIC SAFETY SYSTEM INITIATION

5.2 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, 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 safety systems and that the safety case does not need to claim early action by operators to initiate, moderate or disable safety systems. This principle is developed in the following sections. It is subject to application of the overriding ALARP principle.

5.3 DEFINITION OF THE 30 MINUTE PERIOD

5.4 Paragraph 405, in support of SAP ESS.9, states ONR's expectations that there should be a nominal period of approximately 30 minutes, commencing upon the indication of a reactor trip or plant protection signal, within which the safety of the facility should not

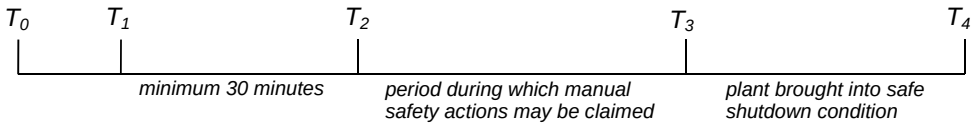
be dependent upon the operator carrying out any control actions which actuate, or contribute towards the control, or effectiveness, of safety systems.

5.5 The 30 minute period stated in 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 conservative deterministic design principle intended 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.

5.6 OPERATIONAL DEFINITION OF THE 30 MINUTE PERIOD

5.7 SAP ESS.13 requires that there should be a means of indicating to the operator that a demand for safety system action has arisen. The point at which the 30 minute period is taken to commence should correspond not to the reactor trip or safety system actuation itself, 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). Thus, a full 30 minute period should be available for the operator to monitor the developing situation 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 344 to design basis events



Key:
T_0: demand for safety system operation
T_1: indication of demand for safety system operation to operator
T_2: point from which manual safety system actions may ordinarily be claimed
T_3: point by which safety system operation must have commenced for facility to be brought to safe (e.g. shutdown) condition
T_4: facility in safe quiescent state

5.8 Figure 1 shows that, following an event which demands safety system operation (T0), the safety system must be brought into operation by time T3 in order for the facility to be brought into a safe state by time T4. Ordinarily, this should be achieved automatically (ESS.8). However, in any event for which operator safety actions are claimed, three separate periods of activity must be considered:

a) the safety case should define the time period T_0-T_1 as, together with T_4 this allows the subsequent periods T_1-T_2 and T_2-T_3 to be defined.

b) operator safety actions should not be claimed to start within 30 minutes of the initiating event being indicated (T_1-T_2). Information about facility status may be gathered during this period, and the safety case should demonstrate that sufficient time is available to gather and interpret the information needed to support the performance of operator safety actions which commence after the 30 minute period.

c) the safety case should demonstrate that claimed operator safety actions after this point are themselves feasible in the time available (T_2-T_3).

5.9 When considering b) and c) above, the Assessor 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 Assessor should ensure that claims on operator safety action are adequately supported (SAPs EHF.5, EHF.7 and Paragraphs 446 and 456). Guidance on the factors to be considered when reviewing such claims is provided in separate TAGs; notably NS-TAST-GD-027 “Training and Assuring Personnel Competence” [8]; NS-TAST-GD-059 “Human Machine Interface” [9], NS-TAST-GD-060 “Procedure Design and Administrative Controls” [10], NS-TAST-GD-061 “Staffing Levels and task organisation” [11] and NS-TAST-GD-062 “Workplaces and Work Environment” [12]. 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.

5.10 PROVISION FOR OPERATOR SAFETY ACTION WITHIN THE 30 MINUTE PERIOD

5.11 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.

5.12 It is sensible to take advantage of the operational flexibility offered by early operator action, so long as this action does not need to be claimed in Design Basis Analysis (DBA) aspects of the safety case and does not have the potential to impair facility safety (paragraph 404). The following principles may therefore be applied:

a) 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.

b) 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 be able to carry out simple and well-rehearsed remedial 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 (Issue E, para 10.9 [6]).

c) Where it is proposed to allow operator action to reinforce or support safety system performance within the 30 minute period, 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). More detailed guidance on the factors to be considered is given in NS-TAST-GD-062 [12], NS-TAST-GD-059 [9] and NS-TAST-GD-060 [10].

d) 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 (i.e., the safety system is responding correctly given a current demand). Nuclear facilities should be designed so that they can accommodate spurious or inappropriate safety system operation. Spurious actuation of safety systems should be avoided by means such as the provision of multiple independent divisions within the design architecture and majority voting . For a complex Class 1 safety system (eg one which is computer-based), every spurious actuation brought about by common cause failure of system components should be analysed as a design basis fault. The fault analysis should assume that the common cause failure also disables all other safety functions provided by the system, but may assume that such disabling does not further exacerbate the fault. (ESS.22 and para 418).

5.13 GENERAL CONSIDERATIONS

5.14 CLAIMS FOR EARLY OPERATOR SAFETY ACTION IN SEVERE ACCIDENTS

5.15 Rigorous application of design basis analysis should ensure that severe accidents are highly unlikely, but suitable and sufficient severe accident analysis is still required to ensure that risks are reduced so far as is reasonably practicable, and to support the facility PSA. Although SAPs ESS8, ESS9 and underpinning paras 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, claims for early operator action to mitigate severe accidents, as referred to in SAPs FA.15 and FA.16, should be scrutinised as appropriate to their importance in line with the general guidance on claims for operator action in NS-TAST-GD-063 'Human Reliability Analysis' [13].

5.16 Although it is appropriate to take a best estimate approach to analysing severe accident fault sequences (SAPs para 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. NS-TAST-GD-063 'Human Reliability Analysis' [13] provides further guidance on consideration of claims for operator actions.

5.17 TREATMENT OF CLAIMS FOR EARLY OPERATOR SAFETY ACTION IN EXISTING CIVIL REACTOR FACILITIES

5.18 SAPs ESS.8, ESS.9 and underpinning paras 404 and 405 should be regarded as general principles against which a facility design is assessed. No exceptions should normally be made for new facilities at the design stage. For existing facilities, however, where cases which do not comply with this principle are encountered, 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 justification of the claim for early operator action which should demonstrate why it is not reasonably practicable to achieve the desired safety system performance automatically. Normally, this should include human factors analysis to describe the claimed operator actions, establish their feasibility and identify potential improvements. Guidance on the factors to be considered when reviewing such claims is in NS-TAST-GD-063 'Human Reliability Analysis' [13], but some of the key expectations are drawn out below:

a) 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. 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.

b) 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 minimised.

c) The licensee should confirm a commitment to carry out regular training which covers the operator's tasks, and monitoring of performance. Particular 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.

6. REFERENCES

1 Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. ONR. November 2014. http://www.onr.org.uk/saps/saps2014.pdf.

2 ONR How2 Business Management System. Human Factors Integration. TNS-TAST-GD-058, revision 3. ONR. March 2017. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

3 ONR How2 Business Management System. Safety Systems. NS-TAST-GD-003. Revision 7. ONR. December 2014. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

4 Licence condition handbook. ONR. February 2017. http://www.onr.org.uk/documents/licence-condition-handbook.pdf

5 ONR How2 Business Management System. ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable). NS-TAST-GD-005, Revision 8, ONR, July 2017, http://www.onr.org.uk/operational/tech_asst_guides/index.htm

6 Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. WENRA. January 2008. www.wenra.org.

7 IAEA Safety Standards, Safety of Nuclear Power Plants: Design. SSR-2/1, Revision 1, IAEA, February 2016. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf

8 ONR How2 Business Management System. Training and Assuring Personnel Competence, NS-TAST-GD-027 , Revision 5, ONR, July 2017. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

9 ONR How2 Business Management System. Human Machine Interface, NS-TAST-GD-059, Revision 3, ONR, November 2016. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

10 ONR How2 Business Management System, Procedure Design and Administrative Controls, T/AST/060, Revision 2, ONR, November 2014. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

11 ONR How2 Business Management System, Staffing Levels and Task Organisation, NS-TAST-GD-061, Revision 3, ONR, March 2017. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

12 ONR How2 Business Management System, Workplaces and Work Environment, NSTAST-GD-062, Revision 3, ONR, February 2017. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

13 ONR How2 Business Management System, Human Reliability Analysis, NS-TAST-GD-063, Revision 3, ONR, April 2015. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

7. GLOSSARY AND ABBREVIATIONS (EXAMPLE LIST)

ALARP	As low as reasonably practicable
DBA	Design Basis Analysis
HF	Human Factors
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
ONR	Office for Nuclear Regulation
RGP	Relevant Good Practice
SAP	Safety Assessment Principle(s)
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association