Office for Nuclear Regulation

ONR GUIDE			
Safety Related Systems & Instrumentation			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-031 Revision 6		
Date Issued:	September 2018	**Review Date:**	April 2023
Approved by:	Steve Frost	E,C&I Professional Lead	
Record Reference:	CM9 Folder 1.1.3.978. (2020/261269)		
Revision commentary:	Rev 5: Routine update Rev 6: Updated Review Bits		

TABLE OF CONTENTS

1. INTRODUCTION 2
2. PURPOSE AND SCOPE 2
3. RELATIONSHIP TO LICENCE CONDITIONS AND OTHER RELEVANT LEGISLATION .. 3
4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED 4
5. ADVICE TO INSPECTORS 4
6. FUNCTIONAL DESIGN REQUIREMENTS – BASIC PROCESS OR PLANT CONTROL, COMMUNICATIONS AND SERVICES. 5
7. FUNCTIONAL DESIGN REQUIREMENTS – RADIOLOGICAL MONITORING INCLUDING CRITICALITY INCIDENT DETECTION 9
8. DESIGN FOR RELIABILITY, RELIABILITY CLAIMS AND FAILURE MODES 11
9. LAYOUT AND VULNERABILITY TO INTERNAL/EXTERNAL HAZARDS 13
10. QUALIFICATION, TYPE TESTING AND STANDARDS 15
11. IN-SERVICE EXAMINATION, INSPECTION, MAINTENANCE AND TESTING (EIM&T), LIFE LIMITING FEATURES AND OBSOLESCENCE 17
12. REFERENCES 20
13. GLOSSARY AND ABBREVIATIONS (EXAMPLE LIST) 21
14. APPENDICES 22

Published 09/18

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 The Office of Nuclear Regulation (ONR) has the responsibility for regulating the safety of nuclear installations in Great Britain. The Safety Assessment Principles (SAPs) for Nuclear Facilities [1] provides a framework to guide regulatory decision-making in the nuclear permissioning process. The SAPs are supported by Technical Assessment Guides (TAGs) which further aid the decision-making process.

2.2 This TAG provides guidance to aid Inspectors in the interpretation and application of SAPs related to, the assessment of nuclear licensees' safety submissions in the area of Safety Related Systems (SRS) and Safety Related Instrumentation (SRI). The broad class of systems that comprise SRS and SRI are defined and discussed. The close relationship between SRS, SRI and Safety Systems (SS) is explored, and the associated Safety Assessment Principles explained. As for all guidance, inspectors should use their judgment and discretion in the depth and scope to which they apply this guidance.

2.3 Nuclear facilities use a variety of systems concerned with safety. At the highest level of importance there are the safety systems. Safety systems are provided to detect potentially dangerous plant failures or conditions and to implement appropriate safety actions, i.e. they are systems that respond to a fault to prevent or mitigate a radiological consequence, and incorporate protection systems, safety actuation systems and the essential services that provide support. These systems generally contribute to levels 3 to 5 of a defence in depth concept (SAP para. 152).

2.4 Besides the safety systems identified above there are other systems, known as safety-related systems (SRS) that, perform an operational function but which also provide a claimed safety benefit. The control and instrumentation of safety-related systems (which includes the facility control system, indicating and recording instrumentation, alarm systems and communications systems) have a close relationship with safety systems (SAP para. 430).

2.5 The prime purpose of SRIs may be plant operability (e.g. basic process or plant control systems) rather than safety, and where they are used to contribute to levels 1, 2, 4 and 5 of a defence in depth concept (SAP para. 152) it should be justified. SRI is not normally be used for level 3 of defence in depth as at this level safety systems should be used, as necessary, to act in response to a fault.

2.6 The following example illustrates the difference between the instrumentation of a safety related system and that of a safety system:

2.6.1 An undesirable plant state is indicated by two alarms, a 'High' and a 'High High'. If the first, 'High', alarm indicates an undesirable trend or a departure from a preferred level but one that is still within the normal operating envelope then it is a safety related system. Corrective action can be taken by the operator. If the second, 'High High', alarm indicates a fault causing the normal operating envelope to be breached requiring prompt corrective action this would be done automatically by a safety system with an alarm to the operator indicating the protective action taken.

2.7 It should be noted that the differentiation between SS and SRS is based on functionality and not safety integrity such that the designation of a system (ie SS or SRS) depends solely upon what it does, and not upon what safety integrity it is required to achieve. SRI failures may also be the initiating faults of fault sequences.

2.8 This approach recognises that the safety integrity requirements of safety function delivered by either a safety system or safety related system depends upon the risk reduction required in respect of the scale of the hazard such that the greater the nuclear safety significance of the hazard, the higher the safety integrity requirement. This is reflected within the categorisation of safety functions (SAP principle ECS.1), and classification of structures systems and components that deliver those functions (SAP principle ECS.2). There is no explicit linkage between functionality and category or class.

2.9 The term 'safety integrity' is used in preference to 'reliability', to indicate inherent robustness, systematic integrity and fault tolerance as well as hardware reliability. Reliability on its own relates to the rate of failure, which is dependent on the environment as well as on the system itself.

3. RELATIONSHIP TO LICENCE CONDITIONS AND OTHER RELEVANT LEGISLATION

3.1 This guidance relates in particular to the following licence conditions [2];

3.1.1 LC11 (Emergency arrangements),

3.1.2 LC14 (Safety documentation),

3.1.3 LC15 (Periodic review),

3.1.4 LC17 (Management systems),

3.1.5 LC23 (Operating rules - limits and conditions in the interests of safety),

3.1.6 LC27 (Safety mechanisms, devices and circuits),

3.1.7 LC28 (Examination, inspection, maintenance and testing),

3.1.8 LC34 (Leakage and escape of radioactive material and radioactive waste)

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

4.1 This guide identifies relevant SAPS and provides further explanation where appropriate. Functional and integrity requirements of safety related instrumentation arise both as direct and inferred requirements throughout the SAPs as well as in the specific engineering principles (ESR.1-10) and related paragraphs. This technical assessment guide is based on the 2014 Edition Revision 0 SAPs [1].

4.2 The guidance has been arranged to cover the following topics:

4.2.1 Functional design requirements – basic process control, communications and services;

4.2.2 Functional design requirements – radiological monitoring and criticality incident detection;

4.2.3 Design for reliability, reliability claims, and failure modes;

4.2.4 Layout and vulnerability to internal/external hazards;

4.2.5 Qualification, type testing and standards; and

4.2.6 In-service examination, inspection, maintenance and testing (EIM&T), life limiting features and obsolescence.

WENRA Reactor Safety Reference Levels

4.3 The objective of The Western European Nuclear Regulators Association (WENRA) is to develop a common approach to nuclear safety in Europe by comparing national approaches to the application of International Atomic Energy Agency (IAEA) safety standards.

4.4 The guidance in this TAG is consistent with the following harmonisation issues from the WENRA Reactor Safety Reference Levels [3], which represent good practices in the WENRA member states, are relevant and should be taken into account by the inspector:

Issue G: Safety Classification of Structures, Systems and Components.

IAEA Safety Standards

4.5 The guidance is also consistent with the following IAEA safety requirements and guidance:

SSG-39: Design of Instrumentation and Control Systems for Nuclear Power Plants, 2016 [4].

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

5. ADVICE TO INSPECTORS

5.1 Advice to inspectors is included under each relevant SAP in the following sections.

6. FUNCTIONAL DESIGN REQUIREMENTS – BASIC PROCESS OR PLANT CONTROL, COMMUNICATIONS AND SERVICES.

Engineering principles: control and instrumentation of safety-related systems	Provision in control rooms and other locations	ESR.1
Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations.		

6.1 The provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents. The equipment should include indicating and recording instrumentation and controls as appropriate.

Engineering principles: safety systems	Monitoring of plant safety	ESS.3
Adequate provisions should be made to enable the monitoring of the facility state in relation to safety and to enable the taking of any necessary safety actions during normal operational, fault, accident and severe accident conditions.		

6.2 Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made in a central control location and at emergency locations (preferably a single location for a reactor) that will remain habitable during foreseeable facility or site emergencies (SAP para. 400).

Engineering principles: human factors	User interfaces	EHF.7
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.		

6.3 This principle applies to central control rooms, local plant control stations, locations where maintenance and/or testing is carried out and locations identified for monitoring or control within a facility's emergency preparedness and response arrangements (eg site emergency control centres) (SAP para. 453).

6.4 User interfaces, which may be analogue or digital, include controls, indications, alarms, recording instruments, overview displays, mimics, communication equipment, computer-based procedures, computerised operator support systems, intelligent decision aids and reconfigurable displays and controls. Additionally, plant equipment such as valves, emergency supply connection points and similar plant and equipment may also be considered as user interfaces (SAP para. 454).

6.5 User interfaces (SAP para. 456) should:

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

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

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

6.5.4 support effective diagnosis of plant deviations;

6.5.5 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;

6.5.6 support communication between personnel located in the same or different operating locations, including locations external to the facility or site; and

6.5.7 be clearly labelled (SAP para. 455).

6.6 The aim here is to ensure that relevant information about a plant is brought together in a convenient location to provide operators with as complete a picture as possible of plant status and behaviour to facilitate decision making, and similarly to bring together appropriate means of control to allow quick and coordinated action in the interests of safety.

6.7 An emergency control/monitoring station should also be provided to permit safe control in the event of the central control room having to be evacuated.

6.8 The provisioning should derive from a systematic analysis of the essential monitoring and control needed to achieve and maintain a safe plant.

6.9 Where it is not possible to carry out certain plant controls from a central location (e.g. manually operated valves), then information relevant to the particular control should be available on the plant to assist the local operator.

6.10 Reference should also be made to the assessment guide [5] that deals with relevant human factors aspects, including the role of personnel (including allocation of function between personnel and automatic systems); user interface; working environment; and quantitative human reliability assessment.

6.11 The accident management strategies should include provision of appropriately robust, suitable and sufficient instrumentation for monitoring the facility and site in accident conditions. The design and location of the in-situ instrumentation should be informed by severe accident analysis (SAP para. 778). Where additional hardware would facilitate accident management, this should be provided if reasonably practicable (SAP para. 779).

6.12 The reference to accident conditions is particularly relevant for systems and instrumentation specified to perform post-accident monitoring or controlling functions. It is essential that such instruments are able to withstand without degradation of their essential functions the worst case conditions that the accident can cause. The extremes of environmental conditions under which claimed SRS are required to operate reliably should be determined, and alarms or other indications provided to alert operators to their being approached and then exceeded.

Engineering principles: safety systems	Demonstration of adequacy	ESS.11
The adequacy of the system design to achieve its specified functions and reliabilities should be demonstrated for each safety system.		

6.13 Any safety-related systems that contribute towards reducing the risk from each initiating fault and/or the overall protection claim should be included in a 'fault schedule' (also known as a safety schedule or a fault and protection schedule) that links faults, fault sequences and safety measures. The schedule should include all relevant initiating faults with their frequencies and consequences (SAP para. 407).

Engineering principles: control and instrumentation of safety-related systems	Performance requirements	ESR.2
The reliability, accuracy, stability, response time, range and, where appropriate, the readability of instrumentation, should be adequate for it to deliver its safety functions.		

6.14 The need for this SAP is largely self-evident. It serves to remind the assessor of the various characteristics of the instrumentation of safety-related systems that need to be individually considered and questioned if necessary.

Engineering principles: control and instrumentation of safety-related systems	Provision of controls	ESR.3
Adequate and reliable controls should be provided to maintain all safety-related plant parameters within their specified ranges (operating rules).		

Engineering principles: control and instrumentation of safety-related systems	Response of control systems to normal plant disturbances	ESR.9
Control systems should respond in a timely, reliable and stable manner to normal plant disturbances without causing demands on safety systems.		

6.15 Although safety is primarily vested in safety systems the demand rate upon them nevertheless represents a direct contributor to the resulting accident frequency. The above two SAPs seek to restrict that demand frequency by ensuring that control systems are designed to cope reliably with normal disturbances without demanding safety system action.

Engineering principles: control and instrumentation of safety-related systems	Minimum operational equipment	ESR.4
The minimum control and instrumentation in each of the facility's permitted operating modes should be specified (operating rules) and its adequacy substantiated.		

6.16 Where safety depends upon information then the systems that provide that information should be listed and the licensee's arrangements shown to prohibit operation without an appropriate minimum set.

Engineering principles: control and instrumentation of safety-related systems	Communications systems	ESR.7
Adequate communications systems should be provided to enable information and instructions to be transmitted between locations on and, where necessary, off the site. The systems should provide robust means of communication during normal operations, fault conditions and severe accidents.		

6.17 These communication systems should be designed to not have any adverse effect on safety systems, or other safety-related systems (SAP para. 434).

6.18 It is impractical for all indications and controls to be centrally located for all possible circumstances, so communication systems are necessary linking the parties likely to be involved in maintaining safety. It should be ensured that the communication systems themselves cannot give rise to additional hazards, e.g. interference from mobile phones.

Engineering principles: control and instrumentation of safety-related systems	Power supplies	ESR.6
Safety-related system control and instrumentation should be operated from power supplies whose reliabilities and availabilities are consistent with the safety functions being performed.		

6.19 In the case of monitoring, warning and communication functions, these supplies should be uninterruptible and independent of other safety-related systems (SAP para. 432).

6.20 The function of a safety-related system should not be degraded by its power supply (or any other service). Those safety-related systems whose correct functioning depends upon an uninterruptible power supply or other service should be identified and the supply provisions shown to be appropriate.

6.21 Supplies to safety-related systems may also be provided from 'essential services'. The services may include electricity, gas, water, compressed air, fuel and lubricants, and may need to satisfy two requirements. The first requirement is to provide a guaranteed, or non-interruptible short-term supply to ensure continuity until the long-term essential supply is established, and the second is to ensure that there is adequate capacity to supply the service until normal supplies can be restored (SAP para. 436).

6.22 Safety assessment principles EES.1-9 relating to the capacity, duration, reliability and functional requirements for essential services apply and are additional to the safety system and safety-related instrumentation principles.

6.23 More detailed guidance is given in the relevant assessment guide [7].

Engineering principles: external and internal hazards	Fire detection and fighting	EHA.16
Fire detection and fire-fighting systems of a capacity and capability commensurate with the worst-case design basis scenarios should be provided.		

6.24 The systems referred to in EHA.16 should be designed and located so that any damage they may sustain, or their spurious operation, does not affect the safety of the facility.

7. FUNCTIONAL DESIGN REQUIREMENTS – RADIOLOGICAL MONITORING INCLUDING CRITICALITY INCIDENT DETECTION

Engineering principles: control and instrumentation of safety-related systems	Monitoring of radioactive material	ESR.8
Instrumentation should be provided to detect the leak or escape of radioactive material from its designated location and then to monitor its location and quantity.		

Engineering principles: containment and ventilation: containment monitoring	Leakage monitoring	ECV.7
Appropriate sampling and monitoring systems should be provided outside the containment to detect, locate, quantify and monitor for leakages or escapes of radioactive material from the containment boundaries.		

7.1 Monitoring, recording and alarm systems should be used to report significant deviations from normal operating conditions as an aid to maintaining plant control and detecting leakage (SAP para. 477).

Engineering principles: containment and ventilation: containment monitoring	Monitoring devices	ECV.6
Suitable and sufficient monitoring devices with alarms should be provided to detect and assess changes in the materials and substances held within the containment.		

7.2 The devices and alarms should monitor the physical and environmental conditions important to safety. These devices and alarms should ensure the timely detection, and aid assessment, of unplanned or uncontrolled changes in materials and substances held within the containment. Examples of these may include changes to the quantity, composition, characteristics of volume, radioactivity, fissile content, temperature, and pressure of materials and substances, as well as the presence of explosive mixtures, including gases and vapours that could challenge the containment boundary. Where

appropriate the capability to sample the materials and substances should also be provided (See also SAP para. 469 ff. and SAP para. 530).

Radiation protection	Fault and accident conditions (Emergency Exposure Situations)	RP.2
Adequate protection against exposure to radiation and radioactive contamination should be provided in those parts of the facility that will need to be accessed during faults or as part of accident management. This should include prevention or mitigation of accident consequences.		

7.3 Effective systems should be provided under normal operation and fault conditions for monitoring ionising radiations in the facility to ensure that breakdowns in systems and controls, and long-term changes to radiological conditions, are detected (SAP para. 592).

7.4 Instrumentation should be provided to give prompt, reliable and accurate indication of airborne activity and direct radiation, particularly in operating areas. These should be fitted with alarms to indicate any significant changes in levels necessitating prompt action. The design of this equipment should take into account the required reliability levels and the environmental conditions in which it will need to provide safety functions. Consideration should also be given to the provision of remote indication of radiological conditions following accident situations (SAP para. 593).

7.5 Adequate warning systems (though not necessarily a Criticality Incident Detection (CID) system) should be provided wherever fissile material is present, unless the safety case shows that no criticality excursion could give any individual a whole body dose exceeding the annual whole body dose limit, or that the predicted frequency is acceptably low. An estimate of the criticality consequences should inform the need for the installation of warning systems. Where suitably justified in the safety case, criticality warning systems may form part of a safety system, i.e. be linked directly to the safety measures designed to achieve the safe termination of a criticality incident (e.g. they may directly initiate boron injection) or else trigger an alarm as part of a safety related system (SAP para. 594).

7.6 A CID system is strictly an alarm system and therefore is classified as SRS for the purposes of the application of safety assessment principles.

7.7 The electrical power supply to the CID system should be capable of maintaining effective surveillance and support of its alarm operation for a period sufficient to ensure safety following loss of normal electrical supplies.

7.8 The reliability requirements of the CID system should be specified and justified. Reliability assessments should be provided which demonstrate that the system meets these requirements.

7.9 More detailed guidance is given in the relevant assessment guide [6].

8. DESIGN FOR RELIABILITY, RELIABILITY CLAIMS AND FAILURE MODES

Engineering principles: reliability claims	Measures to achieve reliability	ERL.2
The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.		

8.1 Engineered structures, systems and components should be designed to deliver their required safety functions with adequate reliability, according to the magnitude and frequency of the radiological hazard, and so provide confidence in the robustness of the overall design (SAP para. 178).

8.2 Evidence should be provided to demonstrate the adequacy of these measures. This should include a reliability analysis of both random and systematic failures. Assumptions made in the course of the reliability analysis should be justified (SAP para. 192).

Engineering principles: reliability claims	Form of claims	ERL.1
The reliability claimed for any structure, system or component should take into account its novelty, experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.		

8.3 Adequate reliability and availability should be demonstrated by suitable analysis and data. Where data is inadequate, appropriate measures should be taken to ensure that the onset of failures will be detected, and that the consequences of failure are minimised. Such measures may, for example, include planned replacement after a fixed lifetime or be achieved through a programme of examination, maintenance, inspection and/or testing (SAP paras. 190/193).

8.4 Novel forms or applications of SRI should be avoided if at all possible because of the associated uncertainties in performance. Where novelty cannot be avoided in an SRS however then the above caveats must be applied. See also paragraphs 8.5 and 8.6 of this guide and ESR.5 in relation to computers and programmable devices.

8.5 For modern complex control systems, the avoidance of spurious operation cannot be guaranteed. Therefore major, spuriously initiated failures of control systems should be analysed as initiating faults in the fault analysis (SAP para. 431).

Engineering principles: reliability claims	Margins of conservatism	ERL.4
Where safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the safety case should include a margin of conservatism to allow for uncertainties.		

8.6 This addresses safety related systems that are involved in the initiating faults themselves, when two or more such systems act in combination with each other. ERL.4 is an important principle for application in probabilistic analyses where licensees often seek to take credit for any mechanisms that can reduce the likelihood of a fault developing into an accident. However, because of its nature, it is often the case that SRI is complex, interlinked with other systems, and less controlled with respect to availability than safety systems. Hence there are usually significant uncertainties

involved in assigning appropriate numeric values for reliability. Systems taking credit for multiple SRIs would normally be subject to close scrutiny and require justification as to why SSs or SRSs of appropriate reliability claims are not provided. In fact unless the claim for all contributing elements of SRI taken together in a given fault sequence is clearly pessimistic, and not better than of the order of 1E-1 failures per year in total, the separate SRIs should be treated and assessed as such, e.g. explicit evidence sought with respect to their independence from other systems, from each other, their effectiveness in all the possible circumstances that might occur, their availability when needed, their standard of engineering, and their simplicity.

Engineering principles: design for reliability	**Common cause failure**	**EDR.3**
Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.		

8.7 Usually, safety-related systems tend to be more complex than safety systems and are typically designed to less rigorous standards. Hence special attention should be paid to potential common cause failures, uncertainties in assigned reliability values, availability, and measures to ensure that the system's safety significance will continue to be recognised throughout its life. This is particularly important where claims are made on combinations of safety-related systems (SAP para. 195).

8.8 CCF claims should be substantiated. Where required reliabilities cannot be achieved due to CCF considerations, the safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures (SAP para. 184/187).

Engineering principles: design for reliability	**Redundancy, diversity and segregation**	**EDR.2**
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.		

8.9 It is normally expected that SRI will not be formally claimed in the safety case and, as such, should be typically characterized by a reliability of not better than 10^{-1}/yr or its equivalent for demand based modes. Where SRS is claimed as a modest frequency reduction back-up to a Class 1 safety system covering a Category A Function then it should be demonstrably diverse from the Class 1 safety system for which back-up is required. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function (SAP para. 180).

Engineering principles: control and instrumentation of safety-related systems	Demands on safety systems in the event of control system faults	ESR.10
Faults in control systems and other safety-related instrumentation should not cause an excessive frequency of demands on safety systems or take any safety system beyond its capability limits.		

8.10 An analysis should be provided that identifies the foreseeable ways in which control system faults, including multiple spurious faults or failures on demand, could generate a demand on a safety system (SAP para 435).

8.11 This SAP recognises that control systems themselves represent a threat to safety by their potential for initiating potentially dangerous events under fault conditions. The analysis referred to is necessary to identify such fault conditions so that they can be eliminated by design where possible, the residual fault conditions shown not to be excessive, and potential combination effects of multiple control system faults shown not to defeat the plant safety systems.

8.12 Adequate physical separation and segregation, independence and isolation should be maintained so that no fault in the SRI might jeopardise the safe working of SSs (SAP para. 413, 415) or SRSs.

8.13 Appropriately designed interfaces should be provided between structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class (SAP para. 167). It is important to note that this SAP does not only apply to hardware failures but also to the transmission of data and digital controls. Generally such communications should be from the higher Class system to the lower Class with the reverse prohibited by the use of one way diodes or other isolation devices.

Engineering principles: design for reliability	Failure to safety	EDR.1
Due account should be taken of the need for structures, systems and components to be designed to be inherently safe, or to fail in a safe manner, and potential failure modes should be identified, using a formal analysis where appropriate.		

8.14 Ideally, the structures, systems and components should be fail-safe, i.e. they should have no unsafe failure modes (SAP para. 179).

9. LAYOUT AND VULNERABILITY TO INTERNAL/EXTERNAL HAZARDS

Engineering principles: layout	Access	ELO.1
The design and layout should facilitate access for necessary activities and minimise adverse interactions while not compromising security aspects.		

Engineering principles: layout	Minimisation of the effects of incidents	ELO.4

The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are minimised.

9.1 The design and layout should minimise the effects of internal and external hazards and any interactions between a failed structure, system or component and other safety-related structures, systems or components. It should facilitate access for operation, inspection, testing, maintenance, modification, repair, and event management, and minimise adverse interactions during operational or maintenance activities with other structures systems or components (SAP paras. 224 and 226).

9.2 The need for adequate separation of SRI and their electrical and other service supplies from each other and from other systems and services should be considered to ensure avoidance of vulnerability to all the above sources of SRI failure. This should include 3-dimensional considerations, and also possible use of portable SRI equipment. Physical barriers may be an acceptable alternative to physical separation. This is also an important consideration for SRSs.

9.3 The layout should provide an alternative means of access to facilities and control functions essential to safety that may require local manual intervention (SAP para. 226(e)).

9.4 Support services and facilities, including site communications, important to the safety should be designed and routed so that, in the event of an internal or external hazard or other incident, sufficient capability to perform their emergency functions will remain (SAP para. 227).

9.5 The possible consequences on safety systems and other structures, systems and components important to safety of potential for fire initiation and growth should be assessed in a fire hazard analysis so as to determine the need for segregation and fire resistance (SAP para. 273).

9.6 Structures, systems and components important to safety should be adequately protected against the effects of water (SAP para. 272).

9.7 The effect of a seismic event on the safety of any system or service that may have a bearing on safety should also be taken into account (SAP para. 255).

Nuclear facilities should withstand extreme weather conditions including abnormal wind loadings, wind blown debris, precipitation, accumulated ice and snow deposits, lightning, extremes of high and low temperature, humidity and drought, that meet the design basis event criteria (SAP EHA.11 & para. 257/258). Generally the facility's structures and location of the equipment within the facility should provide adequate protection against such extreme events.

Engineering principles: maintenance, inspection and testing	**Effect of internal/external events**	**EMT.8**
Structures, systems and components important to safety should be inspected and/or re-validated after any event that might have challenged their continuing reliability.		

Engineering principles: external and internal hazards	Electromagnetic interference	EHA.10
The design of facility should include protective measures against the effects of electromagnetic interference.		

9.8 An assessment should be made to determine whether any source of electromagnetic interference either on-site or off-site could cause malfunction in, or damage to, the facility's systems and components, particularly instrumentation (SAP para. 256). (See the relevant assessment guide [8] for detailed guidance on EMC).

Engineering principles: layout	Unauthorised access	ELO.2
Unauthorised access to, or interference with, structures, systems or components or their reference data (including Building Information Modelling (BIM)) should be prevented.		

10. QUALIFICATION, TYPE TESTING AND STANDARDS

Engineering principles: equipment qualification	Qualification procedures	EQU.1
Qualification procedures should be in place to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives.		

10.1 The qualification procedures should demonstrate a level of confidence commensurate with their safety classification (SAP para. 174) and;

10.1.1 address operational, environmental, fault and accident conditions (including severe accidents) (SAP para. 175),

10.1.2 include a physical demonstration that individual items can perform their safety function(s) under the required conditions, and within the time, substantiated in the facility's safety case (SAP para. 176),

10.1.3 ensure that adequate arrangements exist (Licence Condition 6, see the ONR website) for the recording and retrieval of lifetime data covering the item's construction, manufacture, testing, inspection and maintenance to demonstrate that any assumptions made in the safety case remain valid throughout operational life (SAP para. 177).

Engineering principles: maintenance, inspection and testing	Validity of equipment qualification	EMT.4
The continuing validity of equipment qualification of structures, systems and components important to safety should not be unacceptably degraded by any modification or by the carrying out of any maintenance, inspection or testing activity.		

Engineering principles: maintenance, inspection and testing	Type-testing	EMT.3
Structures, systems and components important to safety should be type tested before they are installed to conditions equal to, at least, the most onerous for which they are designed.		

10.2 For components of particular concern and where it is not possible to confirm the ability to operate under the most onerous design conditions, additional analysis should be carried out which utilises available test results and justifies the component's performance and reliability (SAP para. 205).

Engineering principles: safety classification and standards	Codes and standards	ECS.3
Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards.		

10.3 The codes and standards should reflect the functional reliability requirements of the structures, systems and components and be commensurate with their safety classification as discussed in SAP para. 170-173 and SAPs ECS.4 and ECS.5 (SAP para. 169).

Engineering principles: control and instrumentation of safety-related systems	Standards for equipment in safety-related systems	ESR.5
Where computers or programmable devices are used in safety-related systems, evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards.		

10.4 Hardware and software must be subjected to the same standards as other systems commensurate with the level of safety dependence placed upon them. See technical assessment guidance for computer based safety systems TAG46 [Ref. 9]. Because of the uncertainties substantiating computer based systems, conservative limits should be set on the integrity ranges considered claimable from the various standards of the software production process. See also Appendix 1 for a more detailed discussion of computer and other complex and novel technology failure rates; a further assessment guide on computer system requirements is provided [9].

10.5 Evidence should be provided to demonstrate the adequacy of any measures required to achieve reliability claims. This should include a reliability analysis of both random and systematic failures. Assumptions made in the course of the reliability analysis should be justified (SAP para. 192).

Engineering principles: integrity of metal components and structures: highest reliability components and structures	Evidence	EMC.3
Evidence should be provided to demonstrate that the necessary level of integrity has		

been achieved for the most demanding situations identified in the safety case.

10.6 A minor failure in a component or structure that forms a principal role in ensuring nuclear safety should not lead to significant radiological hazard (SAP para. 293).

10.7 In particular, where the construction of instrumentation provides containment functions, then adequate consideration should be given to the design, materials selection, defect control, manufacturing and quality assurance as described in SAPs EMC.1-20 as necessary to ensure that adequate integrity is achieved and maintained.

Engineering principles: integrity of metal components and structures: operation	**Safe operating envelope**	**EMC.21**
Throughout their operating life, components and structures should be operated and controlled within defined limits and conditions (operating rules) derived from the safety case.		

10.8 The parameters of the defined limits should be consistent with the type of component or structure, their potential modes of failure and operational considerations.

11. IN-SERVICE EXAMINATION, INSPECTION, MAINTENANCE AND TESTING (EIM&T), LIFE LIMITING FEATURES AND OBSOLESCENCE

Engineering principles: maintenance, inspection and testing	**Identification of requirements**	**EMT.1**
Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.		

Engineering principles: maintenance, inspection and testing	**Frequency**	**EMT.2**
Structures, systems and components important to safety should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case.		

Engineering principles: maintenance, inspection and testing	**Procedures**	**EMT.5**
Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.		

11.1 Such inspection should be of sufficient extent and frequency to give adequate confidence that degradation will be detected before loss of the safety function (SAP para. 208).

Engineering principles: maintenance, inspection and testing	Reliability claims	EMT.6
Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components (including portable equipment) in service or at intervals throughout their life commensurate with the reliability required of each item.		

11.2 In especially difficult circumstances where this cannot be done, either additional design measures should be incorporated to compensate for the deficiency, or it should be demonstrated that the adequate long-term performance would be achieved without additional measures. Where test equipment, or other engineered means, is used for in-service or periodic testing, maintenance, monitoring or inspection, the extent to which they reveal failures affecting safety functions should be justified. The test equipment, or other engineered means, should be tested at intervals sufficient to uphold the reliability claims of the equipment for which it is claimed to reveal faults (SAP para. 209).

11.3 The carrying out of any maintenance, inspection or testing activity should not unacceptably degrade the validity of equipment qualification for structures, systems and components important to safety (SAP EMT.4).

Engineering principles: maintenance, inspection and testing	Functional testing	EMT.7
In-service functional testing of systems, structures and components should prove the complete system and the safety function of each component.		

11.4 For SRS, examination, maintenance, inspection and testing are a part of normal operation and it should be possible to carry out these tests without any loss of any safety function (SAP para. 210). Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be adopted (SAP para. 211).

11.5 Functional testing of SRI is important to confirm design intent, and tests should apply true in-service conditions where appropriate in order to validate correct operation. For example, a float switch that is tested by forcing the float under the fluid will fail to reveal a sticking float lever. A proper test would lower the fluid level to prove correct operation. When true in-service conditions cannot be applied there must be a dependable and demonstrable relationship between the test conditions and in-service conditions.

11.6 Any functional testing techniques, particularly novel ones such as noise analysis, must be shown to be capable of revealing the failure modes of concern. Every effort should be made during the design stage to ensure that all instruments can be tested and calibrated during operation. Where this is not achievable however, perhaps because of their location, then evidence should be presented to show that they would retain an acceptable performance for the lifetime of the plant.

Engineering principles: ageing and degradation	Safe working life	EAD.1
The safe working life of structures, systems and components that are important to		

safety should be evaluated and defined at the design stage.

11.7 Particular attention should be given to the evaluation of those components that are judged to be difficult or impracticable to replace (SAP para. 213).

11.8 There should be an adequate margin between the intended operational life and the predicted safe working life of such structures, systems and components (SAP para. 214).

Engineering principles: ageing and degradation	**Obsolescence**	**EAD.5**
A process for reviewing the obsolescence of structures, systems and components important to safety should be in place.		

11.9 This principle is more likely to be applicable to systems and components rather than the main structural elements of a facility. The process should identify threats from obsolescence and ensure that an adequate supply of spare parts is available until a solution to any obsolescence issues can be found. The solution will depend on the particular circumstances, but may involve providing alternative components or items of equipment that can carry out the same safety duty, or it may involve redesigning the plant to remove the need for the obsolescent system or components (SAP para. 221).

12. REFERENCES

1 Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. November 2014. *http://www.onr.org.uk/saps/index.htm*

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

3 Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. WENRA. September 2014. www.wenra.org.

4 International Atomic Energy Agency. Specific Safety Guide No. SSG-39 Design of Instrumentation and Control Systems for Nuclear Power Plants. April 2016.

5 Technical Assessment Guide "Human Factors Integration", NS-TAST-GD-058.

6 Technical Assessment Guide "Criticality Warning Systems", NS-TAST-GD-018.

7 Technical Assessment Guide "Essential Services", NS-TAST-GD-019.

8 Technical Assessment Guide "Electromagnetic Compatibility", NS-TAST-GD-015.

9 Technical Assessment Guide "Computer Based Safety Systems", NS-TAST-GD-046.

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

13. GLOSSARY AND ABBREVIATIONS (EXAMPLE LIST)

CCF	Common Cause Failure
CID	Criticality Incident Detector
EIM&T	Examination, Inspection, Maintenance & Testing
IAEA	International Atomic Energy Agency
SAP	Safety Assessment Principle(s)
SRI	Safety Related Instrumentation
SRS	Safety Related System
SS	Safety System
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association

14. APPENDICES

APPENDIX 1: COMPUTER (AND OTHER COMPLEX OR NOVEL TECHNOLOGY) SYSTEM FAILURE RATES

A1.1. Where complex or novel technology is involved in an initiating fault (IF) such that failure properties cannot be accurately predicted by reference to the known failure properties of its component parts, the frequency of the fault should be sufficiently conservative to allow for uncertainties in behaviour. The frequency allocated should be such that operating experience would soon show if it is too low. For example, a control system that is commissioned over a period of 2 years without any observed failure could allocate a frequency of 0.5/yr, on the basis that if the true frequency is significantly higher than this it would have revealed itself during commissioning. Failures observed during commissioning would increase the allocated frequency accordingly. Although the operating profile during commissioning will differ from that during operation (this representing one of the sources of uncertainty), it is felt that the allocation of a reliability value on the above basis gives sufficient pessimism, and has the effect of forcing the main safety dependence to be placed elsewhere.

A1.2. An important point is that averaging of observed faults between a number of IFs needs to be avoided in assigning frequencies in individual fault sequences. For example a control system with 100 actions that is observed to fail once per year is not equivalent to each action failing at a rate of 0.01/yr, since the distribution of failures between the actions cannot be assumed to be equal - or expressed another way - one high frequency fault sequence cannot be compensated for by 99 low frequency sequences - each must be justified individually. Note that this situation is not the same as 100 identical components that exhibit 1 failure/yr overall, since then each component can be assumed to share the failure rate equally because the components are identical. It is more like the situation where 100 different components are observed to exhibit an overall failure rate of 1 per year. Here the individual failure rates are likely to be very different because the components are different. 100 separate actions of a complex control system are best assumed different, even if they have similarities, since the circumstances that can affect their behaviour are numerous.

A1.3. However, having made the above point about assignment of individual IFs for the purpose of determining the level of protection (i.e. number and integrity of Safety Systems) necessary for single fault sequences, where IFs in different fault sequences are equivalent in terms of consequence and level of protection, then it is appropriate to average the data between these faults. This guidance only applies for the purpose of calculating summed accident frequencies not for justifying individual sequence protection. In the above example if the 100 actions represent IFs with the same unprotected consequence and have the same level of protection, then the value of 1/yr could be divided between the 100 in summing the accident frequencies, since for this purpose it does not matter whether all 100 fail at the same rate, just one of the 100 fails every time, or any other distribution of failures in fact occur. Another way of looking at this is that during the 2 years of commissioning, providing no failures have been seen in any of the 100 equivalent actions, then there have been 200 'action years' of experience, and the failure rate assigned per action can legitimately be claimed as 0.005/yr - for summed frequency purposes only. It is important to note that the above only applies to the outputs actions that can cause an initiating event. A general count of Inputs and Outputs (I/O) should not be applied as many modern Distributed Control Systems can have many thousands of I/O. For the purpose of this Summed Frequency Accident analysis this count must be restricted only to those outputs that can cause the initiating event.

A1.4. Although the above analysis is quite complicated to explain and carry out the logic behind it is simple. It is that single fault sequences initiated by IFs involving complex technology should be sufficiently protected to allow for the particular IF to behave as a

'rogue', since it might well do so; but that it is not reasonable to assume that all IFs will behave as rogues.