Office for Nuclear Regulation

ONR GUIDE			
Safety Related Instrumentation			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-031 Revision 4		
Date Issued:	July 2014	**Review Date:**	July 2017
Approved by:	D Senior	Director of Regulatory Assurance	
Record Reference:	TRIM Folder 1.9.3.764 (TRIM 2014/237393)		
Revision commentary:	Revision 4		

TABLE OF CONTENTS

1. INTRODUCTION 2
2. PURPOSE AND SCOPE 2
3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION 3
4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED 4
5. ADVICE TO INSPECTORS 5
6. FUNCTIONAL DESIGN REQUIREMENTS – BASIC PROCESS 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 10
9. LAYOUT AND VULNERABILITY TO INTERNAL/EXTERNAL HAZARDS 13
10. QUALIFICATION, TYPE TESTING AND STANDARDS 14
11. IN-SERVICE EXAMINATION, INSPECTION, MAINTENANCE AND TESTING (EIM&T), LIFE LIMITING FEATURES AND OBSOLESCENCE 16
12. REFERENCES 19
13. GLOSSARY AND ABBREVIATIONS 20
14. APPENDICES 21

Published 07/14

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 Instrumentation (SRI). The broad class of systems that comprise SRI is defined and discussed. The close relationship between 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 defense in depth (SAP para. 143).

2.4 Besides the safety systems identified above there are other systems, known as safety-related systems (SRS) that, while having a significant influence on safety, do not have a direct fault sequence termination function. 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. 363).

2.5 The prime purpose of SRIs may be plant operability (e.g. basic process control systems) rather than safety, and they generally contribute to levels 1 and 2 of a defense in depth (SAP para. 143) However SRI can also be used at levels 4 and 5 (for example severe accident monitoring systems and criticality alarms).

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 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 more serious 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.

2.10 There is also a group of systems used for the detection of criticality incidents, i.e. incidents involving the inadvertent accumulation into a critical mass of material that can undergo nuclear fission. A criticality incident detection system is strictly an alarm system that provides an additional layer of safety by causing prompt evacuation of personnel and therefore limitation of doses. Such systems are regarded as sufficiently important to warrant the provision of high reliability systems and are therefore classed as safety-related systems (SAP para. 364).

2.11 It should be noted that ONR has certain responsibilities for the regulation of ‘conventional safety’, and assessors should be alert to conventional hazards during their routine nuclear safety assessment work and react to any significant conventional safety hazards that are identified during this work.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

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

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)

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 systems arise both as direct and inferred requirements throughout the SAPs as well as in the SRI specific engineering principles (ESR.1-10) and related paragraphs. This technical assessment guide is based on the January 2008 revision of the 2006 Edition 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

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 [1], which represent good practices in the WENRA member states, are relevant and should be taken into account by the inspector:

Issue G: Classification of systems based on their importance to safety.

IAEA Safety Standards

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

NS-G-1.3: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, 2002 [3].

4.6 The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2006 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 SAP in the following sections.

6. FUNCTIONAL DESIGN REQUIREMENTS – BASIC PROCESS 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 locations on the facility.		

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 plant state in relation to safety and to enable the taking of any necessary safety actions.		

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 point) that will remain habitable during foreseeable facility emergencies (SAP para. 338).

Engineering principles: human factors	User interfaces	EHF.7
User interfaces, comprising controls, indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring and control of the plant during all plant states.		

6.3 This principle applies to central control rooms, local control stations on the plant and emergency locations that should remain habitable during foreseeable facility emergencies. It also applies to provisions for maintenance and testing (SAP para. 383).

6.4 The user interface provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents (SAP para. 384).

6.5 The user interface should:

6.5.1 enable the operator to determine plant states and the availability, and status, of plant equipment;

6.5.2 provide a conspicuous early warning of any safety-related changes in plant state;

6.5.3 provide the means of confirming safety system challenges and identifying, initiating and confirming necessary safety actions;

6.5.4 support effective diagnosis of plant deviations; and

6.5.5 enable the operator to determine and execute appropriate system actions, including actions to overcome failures of automated safety systems or to reset a safety system after its operation.

6.5.6 be clearly labelled (SAP para. 385/6).

6.6 The aim here is to ensure that relevant information about a hazardous 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 [4] that deals with relevant human factors aspects, including 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 identify any instrumentation needed to monitor the state of the plant and the level of severity of the accident, and any equipment to be used to control the accident or mitigate its consequences. Where additional hardware would facilitate accident management, this should be provided if reasonably practicable (SAP para. 644).

6.12 The reference to accident conditions is particularly relevant for instrumentation with post-accident monitoring or controlling responsibilities. 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 SRI 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 as the means of achieving the specified function and reliability should be demonstrated for each system.		

6.13 Any beneficial safety-related systems involved for each initiating fault and the overall protection claim should be included in a ‘safety schedule’ (also known as a fault and protection schedule) that lists all postulated faults and hazards with unacceptable

consequences. The schedule should include all initiating faults with their frequencies and consequences (SAP para. 346).

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 its required service.		

6.14 The need for this SAP is largely self-evident. It serves to remind the assessor of the various characteristics of the instrumentation 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 variables within specified ranges.		

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 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 seeks 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 for which facility operation may be permitted should be specified 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 and to provide external communications with auxiliary services and such other organisations as may be required.		

6.17 These communication systems should not have any adverse effect on safety systems, or safety-related systems (SAP para. 368).

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 functions being performed.		

6.19 In the cases of monitoring, warning and communication functions, the supplies should be uninterruptible (SAP para. 367).

6.20 Auxiliary services that support components of a system important to safety should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of the safety function.

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

6.22 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. 370).

6.23 Safety assessment principles EES1-9 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.

Engineering principles: external and internal hazards	**Fire, explosion, missiles, toxic gases etc – fire detection and fighting**	**EHA.16**
Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.		

6.24 The systems referred to in EHA. 16 should be designed and located so that they can function correctly in the event of the worst case fire. Additionally the design and location should ensure 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 substances	ESR.8
Instrumentation should be provided to enable monitoring of the locations and quantities of radioactive substances that may escape from their engineered environment.		

Engineering principles: containment and ventilation: containment monitoring	Leakage monitoring	ECV.7
Appropriate sampling and monitoring systems and other provisions should be provided outside the containment to detect, locate, quantify and monitor leakages of nuclear matter from the containment boundaries under normal and accident conditions.		

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. 400).

7.2 Although everything that is reasonably practicable must be done to prevent escape of radioactive materials there remains the possibility that escape might still occur. This SAP recognises this possibility and requires that information be provided to assist in post-accident recovery.

Engineering principles: containment and ventilation: containment monitoring	Monitoring devices	ECV.6
Suitable monitoring devices with alarms and provisions for sampling should be provided to detect and assess changes in the stored radioactive substances or changes in the radioactivity of the materials within the containment.		

7.3 The devices and alarms should monitor safety-related conditions and ensure detection and aid assessment of unplanned or uncontrolled changes in the volume, radioactivity, or fissile content of nuclear substances within the containment (SAP para. 430).

Radiation protection	Accident conditions	RP.2
Adequate protection against exposure to radiation and radioactive contamination in accident conditions, should they occur, should be provided in those parts of the facility to which access needs to be gained. This should include prevention or mitigation of accident consequences.		

7.4 Effective systems should be provided, where appropriate, 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. 482).

7.5 Instrumentation should be provided, where appropriate, to give prompt, reliable and accurate indication of airborne and direct radiation, including activity levels in operating areas, and should be fitted with alarms to indicate significant changes in levels that require prompt action. Such equipment should be capable of providing reliable indications and alarms, taking into account prevailing environmental conditions. Consideration should be given to the provision for remote indication of radiological conditions following accident situations (SAP para. 483).

7.6 Adequate warning systems (not necessarily a Criticality Incident Detection (CID) system) should be provided wherever fissile material is present, unless an assessment 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 the warning system. Where appropriate, a criticality warning system may have an additional function and be linked to safety systems designed to achieve the safe termination of the criticality incident (e.g. it may initiate boron injection), or trigger an alarm (SAP para. 484).

7.7 Safety systems should be provided to deal with criticality incidents in line with the requirements of the principles presented above and they should be the primary defence against such events. However, in many operating situations it is not possible to be confident that all the potential criticality fault sequences have been foreseen and, therefore, that the safety systems will be adequate. A CID system provides an additional layer of safety by causing prompt evacuation of personnel and therefore limitation of consequential dose.

7.8 A CID system is strictly an alarm system and therefore is classified as safety-related instrumentation for the purposes of the application of safety assessment principles.

7.9 The areas from which evacuation is required should be defined. When triggered the CID system should give an audible alarm of adequate strength throughout the whole of that area and should continue to sound until manually reset. The reset facility should be located outside the evacuation area and access restricted to authorised personnel.

7.10 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.

7.11 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.

7.12 More detailed guidance is given in the relevant assessment guide [5].

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, to provide confidence in the robustness of the overall design (SAP para. 166).

8.2 It should be demonstrated that the required level of reliability for their intended safety function has been achieved unless it can be demonstrated that the reliability can be achieved by other means (SAP para. 170).

Engineering principles: reliability claims	Form of claims	ERL.1
The reliability claimed for any structure, system or component important to safety should take into account its novelty, the 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 shown to be inadequate, appropriate measures should be taken to ensure that the onset of failure can be detected, and that the consequences of failure are minimised. This may include replacing the component after a fixed lifetime, or dependent on inspection results (SAP para. 176/179).

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 however then the above caveats must be applied. See also ESR5 and its discussion in para **Error! Reference source not found.** in relation to computers and programmable devices.

Engineering principles: reliability claims	Margins of conservatism	ERL.4
Where multiple safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the reduction in frequency should have a margin of conservatism with allowance for uncertainties.		

8.5 This discussion addresses safety related systems that are involved in the initiating faults themselves, when two or more such systems act in combination with each other. ERL4 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 of appropriate reliability 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 as though they were safety systems 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 explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.		

8.6 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 devoted to potential common cause failures, due pessimism in assigned reliability values, availability, and measures to ensure that its safety significance will continue to be recognised throughout its life. This is particularly important where claims are made on combinations of more than one safety-related system (SAP para. 181).

8.7 CCF claims should be substantiated. Where required reliabilities cannot be achieved due to CCF considerations, the required 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. 171/174).

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 important to safety.		

8.8 The expectation for SRI is that the safety claims on such systems should be modest, typically characterized by a claim of not better than 10^{-1}/yr or its equivalent for demand based modes. This means that redundancy and diversity are not required for such systems. Where SRI is claimed as a modest frequency reduction back-up to a Class 1 safety system covering a Category A Function then it must 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. 168).

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 a safety system.		

8.9 An analysis should be provided that identifies the foreseeable ways in which control systems under fault conditions, including multiple control faults, could generate demands on safety systems (SAP para. 369).

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

8.11 Safety systems should share no equipment or services with SRIs and interconnections should be avoided or otherwise be restricted in function to monitoring only. Adequate physical separation and segregation, independence and isolation should be maintained so that no fault in the SRI might jeopardise the safe working of the safety system (SAP para. 352, 354).

8.12 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. 155). 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 important to safety 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.		

8.13 Ideally, the structures, systems and components important to safety should be fail-safe, i.e. they should have no unsafe failure modes (SAP para. 167).

9. LAYOUT AND VULNERABILITY TO INTERNAL/EXTERNAL HAZARDS

Engineering principles: layout	Interaction of plant	ELO.4
The design and layout of all facilities and the plant within them should minimise the effects of internal and external hazards, adverse interactions and facilitate access.		

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 para. 206).

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.

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. 205).

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. 207).

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. 233).

9.6 Structures, systems and components important to safety should be adequately protected against the effects of water (SAP para. 231).

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. 222).

9.8 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. 224). Generally the facility's structures and location of the equipment within the facility should provide adequate protection against such extreme events. Where this is not possible then the SRI will need to be qualified to survive the worst case conditions for claims are made on its operation.

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 internal or external event that might have challenged their design basis.		

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

9.9 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 safety-related equipment or instrumentation (SAP para. 223). (See the relevant assessment guide [6] for detailed guidance on EMC).

Engineering principles: layout	**Unauthorised access**	**ELO.2**
Unauthorised access to or interference with safety systems and their reference data and with safety-related structures and components 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 that are important to safety will perform their required safety function(s) throughout their operational lives.		

10.1 The qualification procedures should demonstrate a level of confidence commensurate with their safety classification (SAP para. 162) and;

10.1.1 address operational, environmental and fault conditions (including severe accidents where appropriate) specified in the design (SAP para. 163),

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. 164),

10.1.3 ensure that adequate arrangements exist (Licence Condition 6, see the HSE 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. 165).

Engineering principles: maintenance, inspection and testing	Validity of equipment qualification	EMT.4
The validity of equipment qualification for 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 severe expected in all modes of normal operational service.		

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, reference data from commissioning or rig testing should be established for comparison against in-service test results (SAP para. 188).

Engineering principles: safety classification and standards	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 standards.		

10.3 The standards should reflect the functional reliability requirements of structures, systems and components and be commensurate with their safety classification as discussed in SAP para. 158-161 and SAPs ECS.4 and ECS.5 (SAP para. 157).

Engineering principles: control and instrumentation of safety-related systems	Standards for computer based equipment	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. In attempting to attain such standards however there are particular difficulties with computer systems, since the means of relating software production standards to system integrity are still immature. In effect, because of these difficulties, conservative limits are set on the integrity ranges considered claimable from the various standards of the software production process. SAP ECS.2 requires all systems to be allocated a safety classification, and SAP ECS.3 sets out the design and construction standards that are appropriate for each safety class. 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 [7].

10.5 Evidence, including quality assurance, 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. 179).

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.		

10.6 A minor failure in a component or structure that forms a principal means of ensuring nuclear safety should not lead to significant radiological hazard (SAP para. 251).

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, safety-related components and structures should be operated and controlled within defined limits consistent with the safe operating envelope defined in 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.		

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. 189).

Engineering principles: maintenance, inspection and testing	Reliability claims	EMT.6
Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components important to safety in service or at intervals throughout plant 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 such measures (SAP para. 190).

11.3 Where test equipment, or other engineered means, is claimed as part of in-service or periodic testing, maintenance, monitoring and inspection provisions, 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. 191).

11.4 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 important to safety should prove the complete system and the safety-related function of each component.		

11.5 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.

192). Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated (SAP para. 193).

11.6 Regular proof testing and calibration of SRI is essential to maintain performance, and tests should apply true in-service conditions where appropriate in order to validate performance correctly. 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.

11.7 Any 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. For example, if the approach is to apply redundancy by provision of multiple systems, many of which represent in-service spares, then sufficient should be incorporated at plant build to allow generously for failures during life, and the minimum number and locations of operational instruments to maintain adequate detection capability for which the plant will be permitted to operate should be clearly established and justified at the outset (see also ESR.4 regarding minimum SRI).

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.		

11.8 Particular attention should be given to the evaluation of those components that are judged to be difficult or impracticable to replace (SAP para. 194).

11.9 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. 195).

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.		

11.10 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. 202).

12. REFERENCES

1. *Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/SAP/SAP2006.pdf.*
2. *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. WENRA. January 2008. www.wenra.org*
3. NS-G-1.3:Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, 2002.
4. Technical Assessment Guide "Human Factors Integration", NS-TAST-GD-058.
5. Technical Assessment Guide "Criticality Warning Systems", NS-TAST-GD-018.
6. Technical Assessment Guide "Electromagnetic Compatibility", NS-TAST-GD-015.
7. 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

CCF	Common Cause Failure
CID	Criticality Incident detector
EIM & T	Examination, Inspection, Maintenance and Testing
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
ONR	Office for Nuclear Regulation
SAP	Safety Assessment Principle(s)
SRI	Safety Related Instrumentation
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 (this in fact corresponds to a confidence level of 63% using the Poisson distribution). 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 must 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, BUT ONLY FOR THE PURPOSE OF CALCULATING SUMMED ACCIDENT FREQUENCIES, NOT FOR THE PURPOSE OF 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) must 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 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.