Office for Nuclear Regulation

ONR GUIDE			
Safety Systems			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-003 Revision 7		
Date Issued:	December 2014	**Review Date:**	December 2017
Approved by:	D Senior	Programme Director, Regulatory Assurance	
Record Reference:	TRIM Folder 1.1.3.776. (2016/323002)		
Revision commentary:	Fit for purpose review		

TABLE OF CONTENTS

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 Safety Systems represent a central pillar of the 'Defence in Depth' safety philosophy that is insisted upon in UK nuclear plants. The main aim of this philosophy is to avoid situations where an initiating fault can lead directly to an accident with nothing able to prevent it. Although faults cannot be prevented, provisions (engineered systems and/or procedures) can be deliberately put in place to recognise and respond to faults to prevent and/or mitigate the accident that would otherwise ensue (i.e. they provide protection against those faults). Such provisions are known as Safety Systems (SSs).

2.2 The aim of this guide is to interpret and amplify the Safety Assessment Principles (SAPs)[1] in relation to Safety Systems, in order to advise and inform ONR inspectors in the exercise of their professional regulatory judgement concerning Safety System need and adequacy. As for all guidance, inspectors should use their judgement and discretion in the depth and scope to which they apply it.

3. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS, IAEA AND OTHER STANDARDS

ONR's SAPs and the WENRA reference levels were re-issued in 2014. This TAG will be updated to reflect these changes in due course and in the meantime inspectors need to check that they are using the correct versions of those publications during their assessments.

3.1 This guide elaborates on relevant SAPs where they are not self evident. References to Safety Systems are scattered throughout the SAPs, so Safety Systems are addressed indirectly in many locations as well as specifically in their own section of the SAPs (paras 336 to 362 inclusive, covering SAPs ESS1 to ESS27).

3.2 Much of the advice contained herein is also reflected in Ref 9 - BS IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems. The scope of that standard is wider than this guide, covering in detail all lifecycle aspects (safety management, planning, risk and hazard analysis, validation, commissioning, decommissioning etc) and includes both Safety Systems and Safety Related Systems, although they are both referred to as Safety Related Systems in the standard. Specific references to this standard are not made in the text as they would be too numerous.

3.3 The IAEA Safety Guide that is most relevant is Ref 12 - NS-G-1.3 - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. This is a detailed guide that is provided for system design purposes, including both safety systems and safety related systems, and incorporates comprehensive advice. Cross references to particular sections of the IAEA guide are provided throughout this guide.

3.4 Explicit linkages between relevant sections of this guide and related WENRA Reactor Reference Levels are tabulated in Appendix 4. Other WENRA Reference Levels are not related to the topics in this guide.

4. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

4.1 Licence conditions 14 and 15 (preparation and review of safety cases) apply particularly, and also of relevance are LCs 23 (limits and conditions in the interests of safety), 24 (operating instructions), 27 (safety mechanisms, devices and circuits) and 28 (examination, inspection, maintenance and testing).

5. ADVICE TO ASSESSORS

5.1 Definitions and their Implications

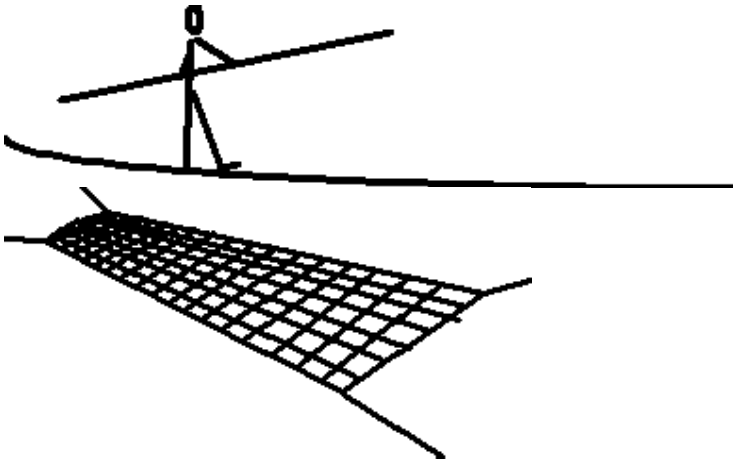
1) 'Safety System' is an IAEA term comprising 'Protection Systems', 'Safety Actuation Systems', and 'Safety System Support Features', and together with 'Safety Related Systems' makes up 'Items Important to Safety' [Ref 12 sections 2.18 et seq. & Fig 1]. The SAPs' definition remains the same as in the 1992 edition of the SAPs, and is 'A system which acts in response to a fault to prevent or mitigate a radiological consequence'. The IAEA definition is similar, but restricted to reactors and aimed at safe shutdown, residual core heat removal, and limiting consequences of anticipated operational occurrences and design basis accidents. The SAPs' definition is more appropriate for use in UK nuclear facility regulation, since such facilities are not restricted to reactors. There are a number of points to consider which are either implied by or can be deduced from the SAPs' definition:

i) It represents a purely functional definition, there is no implied standard of reliability or robustness.

ii) Being a functional definition all aspects of the system that are required to carry out the safety function become encompassed within the definition. These include all elements for

a) detecting the fault condition;
b) carrying out any decision making processes;
c) acting to prevent the accident; and
d) providing any supporting services where failure of the service can impair the safety function (e.g. where the support service does not fail safe). Procedures such as maintenance, testing and calibration also represent supporting services.

iii) A SS is required to act in response to a fault, i.e. when something has gone wrong (e.g. an interlock that prevents a shield door opening when high gamma is present is responding to the fact that high gamma exists at a time when the door is attempting to be opened - i.e. something must have gone wrong for the condition to have arisen), hence it has no role in normal operations. A corollary of this is that removal of the system's safety function (which may or may not be the same as removal of the system as a whole) will not interfere with normal operations. This is an aspect that can be used as an indicator when there is doubt as to the correct classification of a system as a SS.

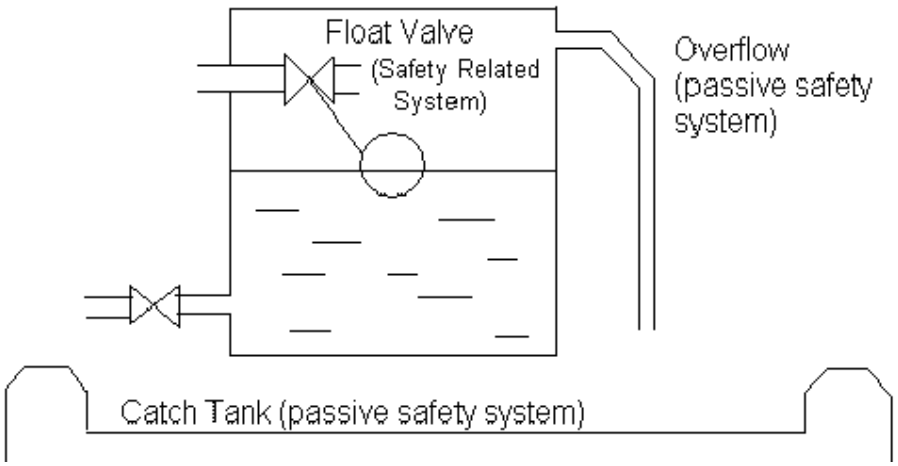


Removal of the safety system (the net), does not interfere with normal operations (walking the tightrope).

iv) A special case arises where response to the fault is to replace like with like and hence preserve the original operational status of the plant, e.g. the automatic cut-in of a reserve ventilation fan. Although strictly this is permitted by the definition of a SS it is preferable to regard it as a plant control (i.e. a safety-related) action. The reason is that otherwise the anomalous complication emerges that there are two (or more) identical items of equipment on plant, one classified as safety related (the first fan), and the other as a safety system (the standby fan). If both fans are regarded as elements of a redundant control system then the situation is more in line with common sense. In these cases the associated safety function would be that which secures the safe state of the plant in circumstances when its basic operational mode can no longer be maintained (in the example, when all the provided ventilation fans have failed). This example relates to ventilation systems that are in use during normal operation. Where ventilation is only used in response to a fault then all parts should be regarded as safety systems and no anomaly arises.

v) Although it 'acts', it is convenient to interpret this term broadly so as not to exclude systems which carry out their function passively, e.g. structures, sumps, containments etc. It is appropriate to classify such systems as SSs if they are able to prevent an accident in response to a fault. In these cases they can be considered to 'act' by bearing without failure the additional stresses imposed by the fault.

For example:-



vi) SAP ESS19 & associated para 353 do not prohibit other functions being carried out in addition to the fault response function, although singleness-of-purpose is the very strong preference. When additional functions are present it is important to focus on the safety function, and the elements of the overall system that deliver it, and to assess the potential for any of the non-safety functions to interfere with it. The more integrated the non-safety functions, the more likely that their faults will impact on the safety function, and the lower the reliability of the system as a result. The same applies if two or more safety functions are integrated in a single system. Here the same concerns arise with respect to one safety function interfering with another.

vii) Since a system can be implemented manually or automatically human involvement is not excluded by the definition. However if human action is involved then there will be additional human factors considerations. In keeping with modern safety practice engineered systems are preferred to administrative systems where reasonably practicable. (See also Ref 12 6.1 et seq. and the assessment guides on 'Human Factors'[3] and Early Initiation of Safety Systems[4]).

viii) Since a requirement of a SS is response to a fault, the context of a system has a more direct bearing on its classification than does its type. For example an alarm that operates within the expected operating envelope of a plant parameter and in response an operator takes controlling action is part of the control system, it is not a SS. However an alarm that operates when a parameter exceeds its expected range and in response an operator takes the necessary safety action is a SS. Detailed guidance on alarms is provided in refs 10, 11 and 12 6.57 et seq.

ix) There are other systems that can affect safety, but which fall outside the definition of a SS. These systems are known as Safety Related Systems (SRSs) -

i.e. items important to safety that are not part of safety systems. Thus SRSs, although intrinsically influencing safety, have no specific duty to

provide adequate safety. Indeed a SRS is often a system whose prime function is not safety related, and its classification as a SRS is determined by the fact that its failure could threaten safety by placing a demand on a safety system.

x) Safety Classification, as required by SAP ECS2 - following para 152, is a separate issue to that of system classification as SSs and SRSs. SS and SRS definitions are purely functional, and do not imply any particular level of integrity. Safety Classification on the other hand relates to the consequence of system failure and to the failure frequency requirements placed on the systems in the safety analysis. Hence SSs may be Safety Class 1, 2 or 3, depending on the integrity that is required of them, though they are more often found in Safety Classes 1 and 2 rather than 3, and similarly SRSs may also be Safety Class 1, 2 or 3.

xi) The formal definition itself does not make clear whether a SS represents a single functional element in a redundant or diverse combination that carries out a safety function, or represents the combination as a whole. For the purpose of this guide the term SS will apply to the combination of elements that make up an overall system responding to the safety functional requirement. The minimum requirement for a SS is one functional element however, for a Class 1 SS redundant [Ref 12 4.22] or diverse [Ref 12 4.23 et seq] element will be required. This combination is often referred to as a basket of safety measures. Viewing the SS as the combination of functional elements is necessary as this brings into play the very important systematic measures that distinguishes an ad hoc collection of functional elements from a well designed system. For the purpose of this guide the term SS will be used to represent the combination of equipment that delivers particular safety function.

2) Encompassed within the term 'safety system' are

i) the protection system - the instrumentation which measures (or monitors) plant parameters (or states) and generates safety actuation signals when these parameters (or states) move beyond pre-set limits;

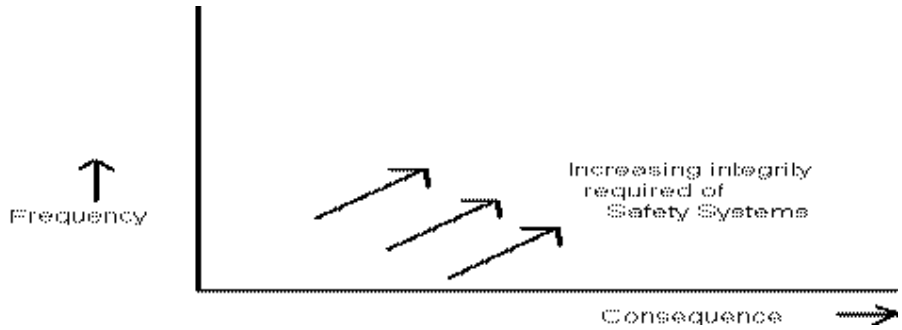
ii) the safety actuation system - the equipment that physically accomplishes the required safety action(s) in response to actuation signal(s) from the protection system; and

iii) the safety system support features - the equipment that provides services such as cooling, lubrication and energy supply to the protection and safety actuation systems [Ref 12 2.18 et seq.].

5.2 Determination of the Need for SSs

1) In identifying the need for SSs, the approach that will be described herein is to determine the potential harm from each individual fault sequence in terms of radiological consequence both on and off site. Reference to other assessment specialisms will be necessary to confirm or otherwise the accuracy of consequence claims in the safety case. For these purposes the effects of any SS or beneficial SRS should be ignored. The presence of substantial items such as passive shielding may however be taken into account providing their presence is guaranteed, their integrity is shown to be invulnerable to the fault

sequence under consideration, and they achieve their safety function simply by being present. This process leads to the concept of the 'unprotected plant', which is the starting point for the analysis.



2) For each fault sequence the frequency of each initiating fault (IF) should be determined ignoring any SS or beneficial SRS. Again reference to other specialisms may be needed to verify the accuracy of safety case claims.

i) For analytical purposes an initiating fault is that which demands protection from a SS. In practice there are often several faults, all of which demand the same protection. It is important to recognise when this is the case and to ensure that the overall frequency used (known as the Initiating Event (IE) frequency) is the sum of all the contributing fault frequencies. The reason for emphasising this point is to avoid the possibility of subdividing a significant IE frequency into multiple component fault frequencies to an extent where they become individually negligible - a practice known as 'salami slicing'.

ii) The protection demand frequency is the frequency of the initiating event reduced by the probability of any naturally occurring conditions that must prevail for there to be a fault sequence. The occurrence of such conditions must not be linked in any way to the event itself. For example the demand 'Processing of a short-cooled fuel rod' consists of the IE 'Processing of a fuel rod' coupled with the condition 'rod selected is short cooled'. The probability of this condition is the number of short cooled rods divided by the total number of rods, and has nothing to do with the event of picking up a rod. An example of an invalid condition would be: Demand - 'Operator enters an active cell', consisting of IE - 'Operator enters cell' coupled with the condition 'Health physics monitor fails to detect activity in cell prior to entry'. Here the monitor's function is carried out because of the impending entry. In this case the IE should be 'Operator attempts to enter cell', and a condition might be 'activity in cell' - being the probability of there being activity in the cell at any random point in time. The monitor's action in this case would be a SS.

iii) Where a potential condition depends upon human activity (e.g. probability of an operator being present in a cell at the time of the IE), or upon some other aspect that might vary over time or with changing operating circumstances, then a generous level of conservatism should be made in the allowance since such variations or changes will occur without triggering a revised safety analysis. The 'point-in-time' risk should also be

calculated for the worst circumstances that might prevail, and protection measures should align with the principles for short term risks as set out in SAP Paras 629 to 638. See also Annex 2 of T/AST/005 [7].

iv) If there is any doubt as to whether a frequency reducing feature should be treated as a condition or as a SS then it should be treated as a SS. The effect of this will be to increase the demand frequency and hence the unprotected risk, but the feature will be included amongst the other SSs in reducing the accident frequency. Hence if the feature is a genuine condition then it will have nothing in common with the SSs and no difference will have been made to the resulting accident frequency. If however it really is a SS, then it might well have elements in common with other SSs and classing it as a SS will force such common elements to be properly considered. Therefore erring on the side of a SS when in doubt is a safer course of action than erring on the side of a condition.

v) Where two things A and B must occur to precipitate a fault sequence then the demand frequency is the sum of (i) the frequency of occurrence of A multiplied by the probability that B has already occurred at that instant, and (ii) the frequency of occurrence of B multiplied by the probability that A has already occurred at that instant. These two components represent the two mutually exclusive situations of A occurring before B, and A occurring after B. Note also that dependencies between A and B complicate the analysis but their effects must be incorporated correctly or the demand frequency is likely to be underestimated.

3) If a value less than 1E-7/yr is obtained for the demand frequency, then subject to satisfying the ALARP principle no special SS is required (but see the note below relating to large releases). This figure is set at 10% of the 'broadly acceptable' risk for offsite consequences of >1Sv (see SAP Target 8) on the basis that a single class of accident should not make a disproportionate contribution to the overall risk (i.e. of the order of one tenth of the frequency in each dose band) - see SAP para 618.

NOTE: SAP Target 9 gives a 'broadly acceptable' risk for large release accidents (>=100 fatalities) of 1E-7/yr. Hence for such accidents, again applying the 10% principle in SAP para 618, the limiting frequency for a single class of accident should be 1E-8/yr.

4) If a value above 1E-5/yr is obtained for an internal demand frequency, or above 1E-4/yr if the demand is due to an external event (see SAP para 514), then, depending upon the potential consequences, the fault sequence might lie within the design basis. In this case, in addition to the other requirements set out below, the safety systems are expected to meet the single failure criterion (SAP EDR4 - following para 174) [Ref 12 4.15 et seq.], and should be analysed in accordance with the design basis analysis SAPs (paras 512 - 526). Design Basis Analysis (DBA) should be regarded as a means of focusing attention on potentially significant faults in order to allow demonstration of design robustness and fault tolerance. Failure to comply with the DBA principles does not necessarily imply unacceptability therefore. However in cases of non-compliance the licensee should provide a robust justification for the particular fault sequence, and show that all reasonably practicable steps have been taken

to avoid unacceptable consequences. DBA and Probabilistic Safety Analysis (PSA) are both essential and complementary. DBA establishes, by conservative analysis, robustness of defence for significant faults that can reasonably be expected to occur during the lifetime of the plant; and PSA establishes, by best-estimate analysis, a comprehensive risk profile for the plant as a whole with respect to predicted behaviours of the plant, its systems, and operators.

5) If the unprotected risk from an individual fault sequence is unacceptable, whether or not it lies within the Design Basis, then SSs should be provided as indicated below to satisfy the ALARP principle and:

i) bring the accident frequency below one tenth (see SAP para 618) of the relevant summed risk frequency listed in SAP Target 8 for accidents involving the public; or

ii) bring the accident frequency below the relevant frequency listed in SAP Target 6 for accidents involving the workforce.

An additional need is for the sum of all fault sequence frequencies within each dose band to meet the summed frequency requirements of SAP Targets 5 and 8. Even if each fault sequence individually meets the above single accident conditions, the overall plant risk might still be too high, in which case additional SSs are required to reduce it.

6) The target reliability (in terms of failures per demand - fpd) for the SSs for each fault sequence will emerge from application of the guidance in para 4.2 5) above. Depending on the value, and whether or not the fault lies within the Design Basis, the following general qualities should be sought and confirmed as adequate by an appropriate form of analysis. The form and extent of analysis depends heavily on the degree of pessimism that is allowed in the allocation of fpd. If generous and evident pessimism is applied then no more than knowledgeable inspection should be necessary, but if little or no pessimism is allowed then a recognised formal technique such as FMEA should be applied and independently checked. Although fixed points are specified below a sliding scale is intended, with variations allowable based on appropriate justification:

i) For faults outside the Design Basis with SSs requiring an fpd >= 1E-2, a good quality single channel system should suffice.

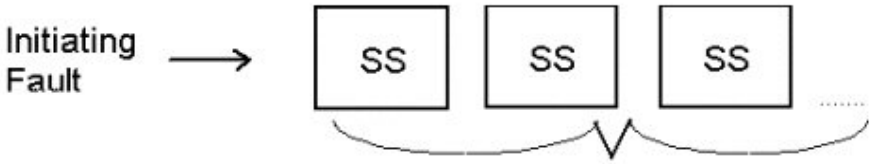
ii) For faults within the Design Basis, or where the SSs require a combined fpd between 1E-2 and 1E-4, there should be at least two redundant means (of comparable reliability) of achieving the safety function. The single failure criterion should be complied with; vulnerability to potential common-cause failures (ccfs) shown to be small in relation to the claimed fpd; services and connections free of common dependencies; adequate segregation from non SSs; and adequate separation between these and other SSs.

iii) For faults where the SSs require a combined fpd between 1E-4 and 1E-6, in addition to the above the redundant means should be diverse,

there should be a detailed common cause failure analysis, and detailed adequacy reviews of services and connections, segregation and separation.

iv) For faults where the SSs require an fpd lower than 1E-6, all the above with increasing numbers of redundant and diverse systems, and increasing rigour in analyses. The difficulties associated with demonstration of very low fpds, especially with respect to ccfs, can be considerable, and dependence on such systems should be designed out wherever possible.

v) For all faults where the SS(s) require an fpd of less than 1E-4 then sole reliance on software-based systems should be avoided[8].



Adequate level of independence difficult to establish for very low fpds

7) Where SSs provide mitigation of the consequences (e.g. evacuation, filtration etc.) rather than prevention, the fault sequence (or its bounding equivalent) should be considered in two (or more for more than one mitigating SS - see note below) parts. Firstly a high consequence sequence ignoring mitigation, where the mitigator is considered in the same way as the other SSs in the subsequent evaluation; and secondly as a low consequence sequence (with the same demand frequency) where mitigation is assumed successful and not considered further, but the other SSs are evaluated in relation to the lower consequence. The reason for these separate sequences is that they give rise to different consequences, and different consequence bands have their own criteria to meet.

NOTE One mitigator requires two fault trees, two mitigators require four fault trees (highest consequence with both subject to failure, two lower sets of consequences, one for each of the mitigators subject to failure separately, and the lowest consequence with neither subject to failure). In general for *n* mitigators there will be 2^n fault trees, although seldom are more than two present in practice. Representation of these multiple mitigator situations is generally clearer if event trees are used.

5.3 Judging the Adequacy of SSs

[Ref 12 5.1 et seq.]

This section discusses a number of specific aspects of SSs and their configuration with guidance about the credit that should or should not be permitted in each case with the associated reasoning.

1) Safety Schedule

i) In order to assess a plant to the SAP criteria a schedule should be provided that lists all postulated faults and hazards with unacceptable consequences. The schedule should include all initiating faults with their frequencies and consequences, the safety systems and beneficial safety-related systems involved for each initiating fault, their categorisation and classification and the overall protection claim. This is the 'safety schedule' (also known as a fault and protection schedule) - see SAP para 346.

ii) It must not be overlooked that SSs can introduce new hazards, particularly when they operate at inappropriate times or in unexpected ways. Hence reliability considerations need to encompass more than merely failure to operate on demand. The assessor should ensure that the licensee has taken account of all credible failure modes that affect safety, and that any additional necessary protection is provided.

2) Requirements Specification correctness

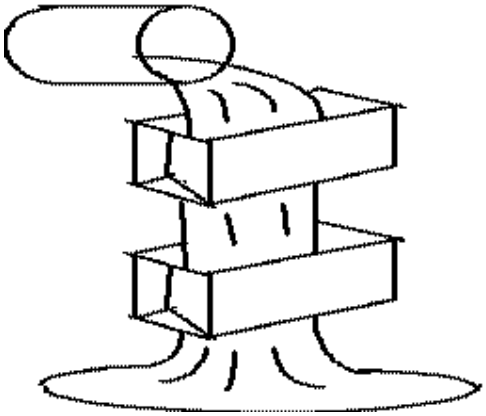
i) A common and easily overlooked source of error is the requirements specification for the system, especially for complex systems where the commissioning procedures cannot be relied upon fully to test all aspects of system behaviour. Particular attention should therefore be devoted to seeking a justification from the licensee for the correctness of the specification for such systems, to give confidence in their ability to deliver the required functionality.

3) Configuration of SSs

i) Dependence on multiple SRSs to reduce the demand frequency on SSs should not be permitted without extreme conservatism, since the reliability and independence of non-purpose designed safeguards is generally very difficult to establish. This is because such systems tend to be more complex than SSs and they are designed to less rigorous standards.

ii) Where multiple low integrity SS are claimed for protection against a fault sequence special attention should be devoted to:

a) potential degradation by common cause failure mechanisms (if the absence of such mechanisms cannot be clearly established then their presence should be assumed);



b) accuracy or due pessimism (where there are uncertainties) in reliability values assigned;

c) guarantees that each SS will not knowingly be out of service at any time that a demand can occur; and

d) measures to ensure that the safety significance of each SS will continue to be recognised throughout life (where several systems are present it is easy to overlook individual systems).

iii) Where credit is claimed for redundancy or diversity, appropriate levels of separation should be shown between each SS, between the services to each SS (unless the SS is shown to be fail-safe with respect to service failures), and adequate segregation between the SSs and other equipment. Additionally the system as a whole should either be shown to be invulnerable to single failures, or the components with single-failure potential should be shown to be reliable and robust enough for their failure contribution not to compromise system unreliability.

iv) Where a SS cannot be shown to be independent of the fault sequence that it safeguards (e.g. by being part of the control system whose failure is a fault initiator), then the potential exists for a single failure both to induce the fault sequence and also to render the SS unavailable. In these circumstances no credit should be allowed for the SS. If a licensee wishes to claim credit then it will be necessary to show that the dependencies are not able to prejudice operation of the SS.

v) Where a SS is integral or shares components with another system that is not a SS, where failure of the other system is not linked with the fault sequence, then the overall complexity is increased and the reliability assigned should be limited to the order of 1E-1 failures per demand unless the licensee can justify otherwise. This is to allow for (a) uncertainties in behaviour due to influences from the other system, and (b) through life changes to the other system that inadvertently affect the SS. Where two independent systems are required to meet the reliability target at least one of them should be free from any other system influence [Ref 12 5.32 et seq.].

vi) The dependence upon non-diverse SSs should be limited to 1E-4 failures per demand, with a justification (for not using diversity) if diversity is not used in support of claims of better than 1E-3 failures per demand. Exceptionally, because of common-cause failure limitations, claims down to 1E-5 failures per demand might be considered for non-diverse systems. In such cases the assessment should take into account the following characteristics: (a) extent of redundancy; (b) component integrity; (c) quantity of known fail to danger modes; and (d) the potential for common cause failure. Additionally any such claim should be supported by a thorough justification. See SAP para 172.

vii) Wherever possible a SS should be implemented by automatic means rather than relying on any human action. Although high integrity human actions can be justified, it is necessary to demonstrate both the necessary high integrity and that this level of integrity will persist throughout plant life. The measures that must be put in place to satisfy these demands are usually very onerous, and a licensee that is inclined to implement manual arrangements in the belief that they will be more economic should be made aware of the continuing demands that will be required. (See also Ref 12 6.1 et seq. and the assessment guides on 'Human Factors'[3] and Early Initiation of Safety Systems [4]).

viii) Assessment of protection adequacy is considerably facilitated by the provision of Configuration Diagrams (or equivalent) that are sufficiently detailed to allow a conceptual understanding of the degree of defence in depth that a licensee is claiming as effective against each fault. Such diagrams should include all safety measures (as defined in the SAPs) that the safety case claims credit for; show the elements of each measure necessary for detection of the fault condition, decision-making, and termination of the sequence; and indicate clearly any mechanisms that may inhibit or degrade the safety function of a measure. Examples of mechanisms that can degrade or inhibit safety functions include operational linkages between measures; components that are shared by two or more measures, or by a measure and other equipment; and electrical supplies or other services where the measure does not fail-safe in the event of its loss.

4) Features of individual SSs

i) For each SS identified in the safety schedule it is necessary for the level of integrity (both in terms of capability and reliability) to be demonstrated in the safety case, although normally only a sample of this information will be assessed by ONR. To assist in this process information should be available that either gives or references, for engineered systems, the following aspects (the level of detail should be commensurate with the integrity level claimed). In each case the licensee is of course free to justify, where appropriate, the absence of any of this information.

ii) Capability aspects: [Ref 12 4.3 et seq.]

a) a system diagram and description;

b) evidence of performance adequacy including range, accuracy, response time, calibration, and margins to the fault study claims [Ref 12 4.54 et seq.],

c) the means provided to maintain, calibrate, test (under operational conditions where possible) and inspect each component (including sensors and actuators); the intervals proposed; and the method of reinstatement after maintenance /calibration /testing /inspection. [SSs should be designed and installed so as to facilitate maintenance and testing etc without excessive dose uptake to operators and without introducing new or increased risks.] Proof tests should be shown to be fully effective for *all parts* of the system involved in delivering the relevant safety function, including any automatic testing or diagnostic test equipment used as part of testing, either during service or during proof test.[Ref 12 4.79 et seq. and 4.97 et seq.] The use of bypasses or vetos during proof testing should be minimised and fully justified. If they are to be used, they should be implemented by properly engineered provisions. (See Appendix 2 for further information);

d) documentary evidence that the system or its components have been qualified or type tested for worst case environmental conditions. (See also Ref 12 4.62 et seq. and 4.77/78 and the assessment guides 'Safety Categorisation and Equipment Qualification'[2], and 'Electromagnetic Compatibility'[5]);

e) evidence that the sensors are capable of detecting the condition for which they are claimed, that the detected parameter represents as directly as possible the variable of concern rather than implying it indirectly [the point here is that the correlation between the measured value and the value of interest should be rigid and dependable, e.g. if flow detection is required then measurement of dp across an orifice plate is acceptable because the dp/flow correlation is dependable, but measurement of pump speed or pump input power would not be acceptable without specific justification. Calculated parameters may be acceptable, but only if there is no direct means of measurement], and evidence of life expectancy if they are not replaceable; and

f) details of bypasses, vetoes, inhibits or intended overrides, if any, with evidence of necessity, demonstration of sound engineering, means and appropriateness of application and removal, and minimisation of human error potential. (See Appendix 2 for further information.)

iii) Reliability aspects [Ref 12 4.8 et seq.]

a) a reliability analysis which addresses both randomly caused and common cause failures. Such an analysis should state the analysis methodology used, the input data and the justification for it (e.g. failure rate data, beta-factors chosen), the test intervals

assumed for component items and any other relevant assumptions (e.g. coverage of in-built diagnostics or self tests, dependence on fault alarms – which may have a common element in otherwise redundant systems);

b) evidence that the system is independent of and invulnerable to any fault (including any cause of any fault) that it is claimed to act against, and independent of and segregated/separated from all other systems;

c) evidence that adequate defences are provided against internal and external hazards, and against dependent failures where redundant or diverse SSs are provided;

d) the means provided to prevent unauthorised access [Ref 12 4.51 et seq.];

e) evidence (if claimed) that the system is fail-safe with respect to failure of services and its own predominant failure modes (See Appendix 3 for further information); and

f) evidence that after SS actuation the plant will remain in a safe state either indefinitely or for an appropriate length of time to bring in reliably other means of maintaining the safe state indefinitely.

iv) Where the SS function is achieved or contributed to by human action then a corresponding justification should be provided to give confidence, commensurate with the level of safety dependence upon the action, in its dependability. (See also Ref 12 6.1 et seq. and the assessment guides on 'Human Factors'[3] and Early Initiation of Safety Systems[4].

v) Safety system actuators should not self-reset after initiation when the parameter exceeded falls back within the acceptable range, but should be reset manually under appropriate administrative controls. Provision should be made to preserve diagnostic information with respect to the cause of the initiation.

vi) Correct and comprehensive commissioning of SSs is necessary for demonstration of both capability and reliability. See assessment guide 'C&I Aspects of Nuclear Plant Commissioning'[6] for further information.

5) Complexity

In general the level of dependence on SSs incorporating complex technology should be limited to the order of 1E-1 failures per demand (interpreted herein as 0.3), unless a sufficiently robust justification can demonstrate the appropriateness of a lower value. See also T/AST/046[8] and Appendix 1.

6) Diagnostics (self-testing)

As systems increase in complexity, especially if they employ software, they generally incorporate a measure of diagnostic capability. The aim here is entirely desirable, i.e. revealing faults in the hardware or in system behaviour to allow action to be taken to prevent hazardous consequences. However there can be undesirable effects in that the level of complexity is increased. The aim should always be that the elements carrying out the diagnostic function, and the diagnostic function itself, should not be able to interfere adversely with the safety function. Provided this criterion is met then the presence of self-testing is beneficial. However if it is not met, for example in systems with embedded software where the processor that implements the safety function also implements the self-tests, then there is a significant danger that the self-test functions can interfere with the safety function. In such cases it is not appropriate to assume that the benefit to safety of self-testing outweighs the disbenefit to safety of increased complexity, and if such a device is to be used then its safety analysis needs to encompass the self-testing software.

In addition, the extent and coverage of diagnostics can be difficult to determine and this may lead to over-optimistic claims of the failures which can be revealed by them (e.g. in terms of the revealed failure rate or detection of anomalous system behaviour). To avoid over-reliance on diagnostics a sensitivity study should be carried out and a conservative claim on their effectiveness demonstrated. It must also be remembered that the diagnostic capability itself must be subject to testing and it may be difficult to demonstrate 100% effectiveness of this test where the diagnostic capability is implemented within the same equipment that it is claimed to be testing.

7) Configuration Management and change controls

Provision should be made for controlling changes throughout the life of the SS in a manner that preserves its integrity. It should be recognised that the change process is itself a significant potential degradation mechanism for the SS, and the integrity of the SS depends heavily on the integrity of this process in terms of the quality of the controls that are applied. Aspects such as configuration management (version control) and impact analysis should receive particularly close attention.

8) Independent assessment

Evidence of independent assessment should be provided for all SSs, the degree of rigour and independence related to the level of safety dependence upon the specific SS.

9) Calculation of summed risk

When all individual fault sequences have been quantified, the frequencies, including those of 1E-7 and below, in each off and on site consequence band (SAP Targets 6 and 8), should be summed and compared with SAP Targets 5 and 8. Significant disparities will require special consideration and possible correction.

10) Operational aspects

i) SS failures should be investigated, and where stressful environmental or operational factors are found appropriate measures should be taken to eliminate them or to make vulnerable components suitably robust.

ii) A through-life monitoring system should be set up to record all failures and causes of failures affecting SSs. Such records should be reviewed periodically to allow improvement where possible and update the predictive estimates of hazard frequency and system unavailability in accordance with achieved performance. [Ref 12 6.63 et seq.]

5.4 Link between System Class and Probabilistic Targets

1) High reliability or low unreliability is linked to the Class of a SS. Generally achieving high reliability or low unreliability requires considerable attention to detail at all stages of a SS lifecycle. With this in mind the following tables show the link between the Class of the system and a range of probability of failure-on-demand (*pdf*) for demand based SSs or SRSs (for nuclear installations the majority of SSs are demand based), frequency-of-failure (*ff*, dangerous failure frequency for high demand or continuous acting SSs or SRSs).

System Class	Probability of failure on demand (*pfd*)
Class 1	$10^{-3} \geq pfd \geq 10^{-5}$
Class 2	$10^{-2} \geq pfd > 10^{-3}$
Class 3	$10^{-1} \geq pfd > 10^{-2}$

System Class	Failure Frequency/yr (*ff*)
Class 1	10^{-3}/yr $\geq ff \geq 10^{-5}$/y
Class 2	10^{-2}/yr $\geq ff > 10^{-3}$/y
Class 3	10^{-1}/yr $\geq ff > 10^{-2}$/y

2) It should be noted that some analyses requires the continuous frequency to be in the form of a rate per hour and in this case a factor of 10000 is usually applied, so, for example, Class 1 would become – 10^{-7}/hr $\geq ff \geq 10^{-9}$/hr. It should also be noted that for complex computer based systems the table in Appendix 3 of T/AST/046 applies. All other safety systems technologies including modern complex programmable logic devices (CPLDs) the above tables apply

6. APPENDIX 1 - A DISCUSSION OF PROBLEMS IN DEALING WITH COMPLEXITY IN SAFETY SYSTEMS

(See also T/AST/046 [8] and Ref 12 4.35 and 5.43 et seq.)

A1.1 It is worth beginning with a source of argument that is believed to lie at the heart of many disputes between licensee and regulator. This is the vital but often misunderstood distinction between dependability and dependence. The dependability of a system is the degree to which it *could be* relied upon, whereas dependence on a system is the degree to which it is relied upon. These sound the same, but only become the same in the unusual circumstance that we are sure of the true reliability of the system. Whenever our knowledge falls short of this, which it always does to a greater or lesser extent, then we must ensure that we place less dependence upon the system than it is capable of bearing. In other words its dependability must always exceed the level of dependence placed upon it. The difference is the safety margin. The important point is that the more uncertain is the reliability *of the particular system in question*, then the greater the safety margin that is required. Such uncertainties abound where advanced systems are used, the greater the complexity and sophistication then the greater the uncertainty in reliability.

A1.2 This causes problems where the regulator insists on regarding *a particular* system as unreliable, in order to establish an appropriate working safety margin, whereas the licensee thinks that it represents the regulator's estimation of the true reliability for that *type of system***.** Note that the use of the word 'system' here relates to the delivery of a single function, for example a single control sequence in a distributed control system. Hence the licensee will argue, quite rightly, that if such systems are as bad as that then they could never be relied upon for anything, and will consider the regulator's view wholly unjustifiable. The regulator's view is subtly different however, and can be summarised as - *even if this particular system is as unreliable as this, which is unlikely but not inconceivable, then adequate safety can still be demonstrated***.** The regulator might add the observation that even though all such systems will not behave so unreliably on average, if the one system that is protecting the fault sequence in question is the one that is so unreliable (the rogue, so to speak), and a higher reliability is assumed, then in the event of an accident it will be of little comfort to point out that ninety-nine other similarly protected accidents might have happened but did not do so!

A1.3 However there still remains an apparent anomaly, in that it will be pointed out that the regulator does not always take so pessimistic a view, for example where a simple hard-wired system is used, even though any individual system might also be a rogue and soon fail. The distinction here is that the 'time-to-failure' distribution of the hard-wired system will be known to a higher level of confidence, so the probabilities of individual times to failure are more accurately known. Furthermore proof tests can be more easily shown to be comprehensive for a simple system, so a failure that does occur can be expected not to persist beyond the next test interval. For complex, especially software-based, systems, where systematic faults are much more likely, the 'time-to-failure' distribution is completely unknown, and the periodic proof tests are unable to reveal other than random faults arising from non-software sources. Hence the level of uncertainty is higher, the safety margin must be larger, and the level of dependence placed on the system should therefore be correspondingly less.

A1.4 There is clearly a potential conflict of interest between advanced technology with its predisposition towards complexity on the one hand and traditional engineering principles which require simplicity on the other. The source of the conflict and its

effects are understandable, but the essential problem still remains. This represents a very important concern in modern systems and it is therefore worth devoting some thought to means by which the required elements of the traditional principles can be retained while still being able to profit from the benefits of advanced technology.

A1.5 If there are such means, then they must be arrived at from a knowledge of what it is that the traditional principles seek to achieve, from a knowledge of what advanced technology can offer, and by deliberate avoidance of degrading the one by the other. It would seem that there should be a solution, since there is nothing intrinsic in the principles that preclude advanced systems per se, although the one difficulty that is most apparent is the objective of avoiding complexity. Let us therefore explore this aspect in more detail.

A1.6 Consider a temperature trip system. The task to be achieved is simple, but if it is to be implemented using a microprocessor then it might appear that unnecessary complexity will be embodied. Considering first hardware aspects in isolation, it is true that a microprocessor is a complex device, so would the requirement for simplicity (see SAP ESS21) preclude it from such an application? To answer this we must consider the particular danger that is perceived in the SAPs by complexity. It is that with a complex system the level of understanding of behaviour is likely to be limited, so that whether or not adequate safety has been achieved might be obscure. Does a microprocessor's hardware complexity give rise to this fear? Not necessarily. Although very few people have an understanding of how a microprocessor performs its function, except in broad conceptual terms, the same can be said of conduction of electricity along a cable. Therefore it can be argued that we need not have complete understanding of the microprocessor hardware in order to have confidence in its capability, any more than we need to understand how a metal conducts electricity to be confident that it does. What is required is confidence, and that can be gained from sufficient experience of reliable behaviour. If a microprocessor is to be used in a trip system, then the level of confidence that is justifiable relates directly to the available experience of performance of the microprocessor in question. Hence we would have more confidence in one that had built a sound track record than one that had only recently been introduced. Care needs to be taken however to ensure that the microprocessor to be used in the safety system is the same as others that have built the track record. Manufacturers often change the physical construction and configuration of particular integrated circuits whilst still delivering the same functionality, so this possibility needs to be taken into account and a design sought that has been stable for some considerable time.

A1.7 Microprocessors, as other systems, suffer from both random and systematic hardware faults, but well established proprietary devices may have an adequate track record in this regard for our purposes *for a single channel*. Remember that we still need to incorporate redundancy and diversity where high integrity is required, and such features defend against these imperfections in microprocessors as they do in non-microprocessor systems. Redundancy defends against random but not systematic faults, and diversity defends against both.

A1.8 If we accept the above reasoning for the hardware, there is still however the software to be considered. Is this simple enough to be relied upon? Here a pertinent point is that unnecessary complexity in the implementation of a task should be avoided. In other words the inherent complexity of a task should not be increased by its implementation. For example a program to read an input port, compare the value with a set point in memory, and to set an output port according to the result can hardly be considered complex from an understanding point of view. Hence it is considered that there is no implicit reason for a microprocessor implementation of a temperature trip system to conflict with the SAPs' requirement for simplicity. We would add that if the task that is to be performed is *itself* inherently complex, then it is probably simpler

to implement it using software than to attempt a purely hard-wired implementation, since methods are well established to develop software for complex applications whereas they are not so well established for non-software designs. We would add however that very few nuclear plant protection functions need have inherent complexity.

A1.9 It is probably worth clarifying this point further since it might appear to contradict earlier remarks about uncertainties in advanced systems. All understanding is hierarchical. We understand a complex thing in terms of the interaction of simpler things that we accept as already understood. In fact the simpler things are often not simple at all, but if we have sufficient prior experience of their dependability in delivering understood functions then they have our confidence, so for our purposes we are justified in regarding them as basic building blocks from which to build an understanding of that which we do not yet have experience of. Understanding, for our purposes, represents in fact a reasoned extrapolation from direct experience. This enables us to generate confidence in the correct functioning of the new system, either before it has built a track record, or even where so high a reliability is required that it can never build a track record. Thus the nature of the simplicity that is sought in safety systems is that which allows a ready understanding of those aspects that are new, i.e. of the *functional design* of the system. For those aspects that are not new, for which experience is available, the degree of dependence should be related to that experience. Hence, although we would be more justified in relying on a wire to conduct electricity than on a microprocessor to carry out a specific set of instructions, arguments based on past experience and simplicity might be successfully used to support a safety case.

A1.10 The temperature trip system described above might be viewed as unrealistic for a software implementation, in that a licensee is likely to seek to incorporate several trip functions within a single microprocessor system (or within a multiplexed communicating microprocessor system). Such incorporation of multiple functions however soon begins to threaten the level of understanding that is required for the necessary confidence. Furthermore it threatens the needed separation of safety systems from each other, and allows the potential for single faults to invalidate several different safety functions at the same time. Also, if, as is likely, common software is used in redundant safety systems, then software faults represent a source of common-cause failure of the redundant implementations of the same safety function. Hence this sort of arrangement conflicts with the need for simplicity in functional design, as well as with several other important safety principles, and for these reasons we would anticipate that the licensee would have a much greater level of difficulty in justifying its safety.

A1.11 It is worth saying something about self-testing however, since this is an eminently desirable feature, but one that again risks increasing the level of complexity. This is an area where constructive thought at the design stage can reduce problems later. Here we have two separate functions, which may or may not be executed by the same processor. The important thing is to engineer these functions so that they remain independent in their actions. Specifically the safety function (e.g. trip), must not be compromised by the secondary function (self-test). The object is to prevent the safety function from being degraded by the self-test program, however complex, by ensuring that control of the safety function never becomes subordinated to the self-test program.

A1.12 In general however we would expect the level of dependence on SSs incorporating complex technology to be limited to the order of 1E-1 failures per demand (interpreted herein as 0.3), unless a sufficiently robust justification either along the above lines or by application of the 'special case' procedure (SAP ESS27) can demonstrate the appropriateness of a lower value.

7. APPENDIX 2 - INTERLOCKS, PERMISSIVES, INHIBITS, VETOES, BYPASSES AND OVERRIDES

[Ref 12 2.21/22 and 5.36 et seq.]

A2.1 Introduction and Definitions

1) Functions referred to as: Safety Interlock, Permissive, Inhibit, Veto, Bypass and Override are often encountered when examining protection and control systems. The functions they represent are implemented as mechanical, pneumatic, electrical and electronic systems. The six terms are used to convey a similar meaning; all imply, 'the prevention, sometimes conditionally, of a course of action continuing or of an automatic system performing its intended function if called upon to do so'. The differences in the functions and their implementation have significant implications for safety. Unfortunately there is considerable inconsistency in the use of the terms. For example a veto on one plant might be referred to as a bypass or an override on another. For the purpose of this discussion the six terms and functions they represent are defined below. These definitions are provided only as an aid to understanding; they are not intended as formal definitions.

i) Interlock - an automatic engineered system used to prevent a hazardous situation occurring by preventing function(s) being initiated unless designated preceding actions have been completed and the necessary safe conditions established. Once the interlock conditions have been met and the action taken the interlock performs no function until challenged again by a request for the action(s) it controls. Interlocks tend to be single function devices but can be made up of a series of simple conditions combined in a binary manner.

ii) Permissive - functionally equivalent to an interlock in that it determines that a particular system state or set of signal conditions exist, before an action can proceed. They are usually implemented as an automatic function in an engineered system by a logical AND of the permissive, which can be a complex decision algorithm, with the signal initiating the action.

iii) Veto - the temporary suspension of function(s), or an item of equipment, using an engineered system, to allow a planned, e.g. maintenance, activity to take place. The application of a veto replaces the output of the equipment under veto to force and maintain the required state – usually the non-trip state. The use of a veto can cause a significant degradation of safety and must therefore be under strict control.

iv) Inhibit - is functionally equivalent to a veto but applied automatically to a function as part of a normal operational procedure that is usually conditional on plant status or mode of operation, i.e. it is an operational veto. For example, this may be conditional logic applied to an interlock function to inhibit the operation of an interlock when it is not required, but when its operation would prevent a legitimate plant operation being carried out.

v) Bypass - prevents the function(s) of an item of equipment by substituting an alternative signal route removing the equipment performing the function(s) from the control or protection loop. A bypass usually forces a desired output state from part of a system, for example to allow continued operation when a system component, such as a sensor or amplifier, has failed, and is one means of applying a veto or inhibit. The provision for a bypass is normally engineered during system design and placed under strict administrative control.

vi) Override - prevention of an automatic action or function by manual action. These are operator actions taken under specific circumstances e.g. as part of an emergency operating procedure; they are neither automatic nor routine functions e.g. maintenance or testing. An override may be used by an operator to prevent an unsafe condition arising because of failures elsewhere on the plant.

2) The functions defined above will be considered in three groups:

i) fully automatic safety actions to maintain safety - interlocks and permissives;

ii) controlled actions to maintain operation - inhibit, veto and bypass; and

iii) unconstrained manual action - override.

3) Interlocks and permissives are permanent features of conditional logic used to provide protection in the event that preceding actions or systems have failed, e.g. a shield door gamma interlock. The systems delivering these functions are classed as safety systems.

4) Inhibits, vetoes and bypasses are used to modify the protection available for operational convenience as:

i) Inhibits - remove complete safety functions;

ii) Vetoes - remove a channel of protection but do not necessarily eliminate the safety functions; and

iii) Bypass - remove an item of equipment but do not necessarily eliminate the safety functions.

These functions affect safety as they can remove or degrade protection and their uncontrolled use must be avoided.

5) Overrides suspend functions and equipment in an 'uncontrolled' manner and should not be available as part of safety systems.

A2.2 Assessment criteria

1) In assessing the safety significance of these differing kinds of function all aspects of their use must be considered; as their application can impact on safety in dissimilar ways. For example, a maintenance veto applied to remove a channel of plant protection from service may also remove the associated electrical supply. In this case the veto provides two somewhat conflicting functions of ensuring worker safety while degrading plant protection.

2) Override facilities are potentially very dangerous as control of their use is basically administrative and their safety is normally dependent on the operator correctly evaluating the situation. The failure of an operator to fully comprehend the current plant state could result in action that creates significant hazard for both the plant and personnel. Further, the change in plant operating regime may not be recognised by those at risk who may take an action and unintentionally exposes themselves to the 'new' hazard.

3) The following points should be considered during assessment of all systems:

i) The reason for the function, its means of implementation and justification.

ii) The equipment providing the required function, or change of function, should be engineered, not provided by temporary modification, e.g. use of jumper leads.

iii) Control over the use of the functions; the level of control will depend on the safety significance of the functions affected.

iv) The control interface of the operator and system performing the function should be arranged to minimise the possibility of error, e.g. unique keys should be used for each function.

v) Arrangements to alert the operator, and ensure continued awareness, of the current status and change of state of all devices.

vi) The effects of inadvertent, incorrect application, or removal of a function. These should be fail safe wherever reasonably practicable.

4) Interlocks and permissives

i) Interlocks and permissives should be applied automatically; proposals for their administrative control should be specifically justified.

ii) The consequences to plant and personnel of the inadvertent introduction or loss of an interlock or permissive should be analysed and additional engineering provided as necessary to ensure that safety is not threatened. The maintenance of safe conditions using procedural means should be justified and considered as a last resort.

iii) An analysis should be performed to determine the safe course of action in the event that the interlock, permissive conditions are lost. The

analysis should consider the safety implication to plant and personnel independently.

5) Inhibit, veto and bypass

i) The engineering arrangements for application of an inhibit, veto or bypass should ensure that the means of connecting equipment to that removed from service, for any purpose e.g. test, repair or calibration, are also engineered and the consequences of connection of that equipment will not propagate beyond the vetoed or bypassed system.

ii) Inhibits, vetoes and bypasses should be applied for the minimum length of time possible.

iii) A maximum time for the application of an inhibit, veto or bypass should be set and, where practicable should be engineered into the system.

iv) The consequences to plant and personnel of the inadvertent loss of an inhibit veto, or bypass should be analysed and additional engineering provided as necessary to ensure safety is not threatened.

v) It should not be possible to veto more than one complete channel of a system.

vi) A veto that reduces a safety system vote to n out of n should not be used.

vii) Vetoes applied to a multichannel system should be applied independently to each channel and not at a single point e.g. the final actuator.

viii) The use of a bypass that eliminates redundancy should be justified.

ix) The operational arrangements for application of an inhibit veto or bypass should be examined to ensure the necessary controls are present. These might include an independent check by a designated person with authority to halt the proposed action.

6) Overrides

i) It should not be possible to override systems that render a plant sub critical or maintain a plant in a subcritical condition.

ii) the application of an override should be prevented by interlocks for those plant modes and signal conditions that would render the override dangerous.

iii) The application of an override to a system designed to maintain cooling or prevent release of radioactive materials should only be possible when it has been demonstrated that there is no other means of avoiding more severe consequences.

iv) The action of an override should be limited to those functions that need to be overridden.

v) The plant operating procedures for the use of overrides should be assessed as this is the only means of controlling their use.

8. APPENDIX 3 - ASPECTS OF FAIL-SAFE DESIGN

A3.1 Introduction

1) For a reliable safety system, besides the avoidance of complexity, a fail-safe approach and the means of revealing faults from their times of occurrence should be applied. It is valuable for the assessor to have a clear understanding of what is meant by the phrases of 'fail safe approach' and 'means of revealing faults' before attempting to discern whether a safety system meets these principles.

A3.2 A fail safe approach

1) The term 'fail-safe' has been used in many engineering disciplines and industries to describe the way in which a system performs when it experiences failure. The term 'fail-safe' should not be equated with 'inherently safe' which implies that the system itself has qualities, or properties, that bestow its performance with safety. An inherently safe system would be one where it is not inherently capable of generating a significantly hazardous event i.e. it lacks the radioactive inventory, or the necessary release energy.

2) The concept of 'fail-safe' as applied in assessment of safety systems encompasses the expectation that when a system fails it would be to a safe state. This means that the failure modes are such that safety would not be prejudiced in the presence of the failure. It also means that careful system design is necessary to engineer that a safe outcome arises from failures. In practice it is very difficult indeed to ensure that all failure modes have a safe effect. The best that can normally be done is to ensure that the predominant failure modes, as well as loss of supplies or services, have safe effects. Note that 'predominant', as used here, does not necessarily mean that most of the failure modes have a safe effect, it means that the most likely failures have a safe effect

3) The 'fail-safe' property engineered into the design of a SS refers to the function that the system performs in relation to the particular hazard(s) which it is provided to protect against. Should a failure of the SS occur there should not be an increase in the plant risk in respect of that hazard. However, it should be recognised that the risk associated with other hazards, against which the SS has not been designed to protect, may be increased as a consequence of the failure.

4) For example the provision of a seat belt in a car has the safety function of restraining a passenger in the event of a collision. The seat belt release mechanism has the potential to fail open and the consequence in a collision would be to fail to restrain the passenger. To overcome this potential hazard

the buckle is made so that its most likely failure modes cause the release mechanism to remain closed, so that for the hazard of a collision the belt fails safe. However, where escape from the car is necessary e.g. fire following a collision, the seatbelt's continuing to restrain the passenger is no longer safe, and therefore for this hazard the seatbelt does not fail safe.

5) Thus, a clear understanding of the safety function of the system is necessary together with knowledge of its failure modes and how they affect the safety function. Often the licensee submits a Failure Modes and Effects Analysis (FMEA) to substantiate the claims made for the reliability of a system and its fail safe design.

6) The assessor should be aware that a rule of thumb used by some licensees in claiming that a system is fail safe is that the safe failure rate should be at least ninety percent of the total failure rate. Assessors need to recognise however that the proportion of safe failures is not in itself a sound measure of adequacy. It may be that a design is adequate where the proportion of safe to total failure rate is considerably less than ninety percent, providing the overall dangerous failure rate (or fpd) is adequately low. Conversely, a design where the safe failure rate is well over ninety percent of the total may not be adequately safe where the overall dangerous failure rate (or fpd) is still too high.

7) Regardless of the licensee's approach fail safety should be considered by the assessor, especially for predominant failure modes and for loss of supplies and services, and a justification sought if such modes are not engineered to produce safe effects.

A3.3 Means of revealing a fault

1) Given that failures can either be safe or dangerous it is important in a reliable safety system that faults of any kind come to light as soon as possible after their occurrence. Thus not only are faults safe or dangerous but they will either be revealed or unrevealed. If a fault was to remain unrevealed for a period of time the plant could be operating in a degraded state of which the operator is unaware. A second fault might arise before the first fault had been revealed, causing a trip if the first fault was safe, or of more concern preventing a trip if the original fault was dangerous. In judging the adequacy of safety systems it is convenient to group the faults as shown below, so that where a design exhibits particular features the appropriate level of justification can be sought.

Grouping of Safe, Dangerous, Revealed and Unrevealed faults

Effect	**Mode**	
	Revealed	**Unrevealed**
Safe	Group I Failures in this group can be considered not to present a threat to the safety function. The failure either has no effect on the safety function or it generates a safety actuation signal. An example of a failure here is associated with the use of a live zero for current loop sensors. Should an open circuit occur the current drops below the live zero level revealing the failure, and initiating the safety function. Fail-safe faults are generally self revealing.	Group II Failures in this group do not prevent a safety function from being carried out, but will become evident only when a specific test or operation necessary to reveal its presence is completed. The availability of the system may begin to be affected. An example here is failure of a switch used to select a veto. The failure in itself does not directly affect the safety function, but will only be revealed when the switch is tested, or the veto needs to be applied and does not work. It is assumed here that a safe state will remain if the veto is not applied.
Dangerous	Group III Failures in this group will partially or totally inhibit a safety function. A benefit is that operators are made aware of the presence of such a fault soon after its occurrence. A justification on whether the failure mode could be eliminated by redesign and the adequacy of the means of revealing the failure should be sought. A similar application of a current loop failure could be envisaged where no safe action is taken once failure has occurred. It would be reasonably practicable to redesign the equipment to make the failure mode fail safe.	Group IV Failures in this group will partially or totally inhibit a safety function without providing any indication at the time that this has occurred. Such failures have to be revealed by deliberate measures to exercise the safety function periodically - i.e. proof testing. These failures are considered to be the greatest threat to the safety function. A single failure of this type in a design may be sufficient to exclude that design from being considered fail safe. An assessor may question whether the failure mode could be eliminated by redesign and why it is not possible to reveal its presence immediately. Such a failure would directly block the safety function while maintaining the appearance that the circuit is healthy. An example is self-oscillation

		in a pulse circuit where the presence of pulses is the healthy condition and the safety function is delivered by removing the pulses. The likelihood of such failures may render a design unacceptable.

2) Thus the types of faults in a safety system have a strong impact on its adequacy. A safety system with only group I and II failure modes is likely to be acceptable (from a safety point of view, though a licensee may reject it from an availability point of view), whereas a safety system with too many group IV failure modes is likely not to be acceptable.

3) The method for revealing failure may well be the activation of the safety function; however this in itself may not be desirable. Usually, an alarm or signal is generated that is logged by other equipment monitoring the safety system. The integrity of the alarm system should be considered and it needs to be shown that an adequate level of isolation has been provided to prevent the alarm system from undermining the integrity of the safety system. Particular attention should be paid to alarms where there is a common element between alarms for redundant (or diverse) equipment– e.g. a common alarm annunciator in a control room for a multi-channel redundant system. The presence of such common elements (i.e. single point failures) can significantly worsen calculated random failure probabilities or frequencies for otherwise separate equipment.

4) Further points also need to be considered:-

i) excessive frequency of fail safe faults can itself become a safety concern: examples include the need to re-start a plant more often (i.e. to exercise a more dangerous operational mode); additional pressures on operators to restore plant operations before the safety system fault has been fully resolved; and the erosion of belief that a safety action is in response to a genuine plant demand;

ii) for faults that cannot be rendered fail-safe the first level fall-back should be to make them revealed at the time of occurrence, or as soon as possible thereafter, commensurate with an acceptable level of risk (an appropriate periodicity of proof testing applies to this latter strategy); another option is to re-engineer the system to reduce the failure frequency or fpd;

iii) the integrity of the revealing system and the manner and circumstances in which it operates needs to be taken into account in the analysis, including consideration of the failure of the revealing system itself; and

iv) staggered (as opposed to simultaneous) proof testing allows earlier detection of common cause failures across redundant channels; the revealing of single channel faults also reduces some failure probabilities where such ccfs do not manifest simultaneously on all potentially affected channels - providing a time of grace, albeit short.

9. APPENDIX 4 - TABLE OF LINKS TO THE WENRA REACTOR REFERENCE LEVELS

Abbreviation: SS - Safety System

WENRA Reactor Safety Reference Levels	T/AST/003: Safety Systems
Issue E - Design Basis Envelope for Existing Reactors	
2.1 Defence-in-depth shall be applied in order to prevent, or if prevention fails, to mitigate harmful radioactive releases. The design shall therefore provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment, and an adequate protection of the barriers.	1.1 "Safety Systems represent a central pillar of the 'Defence in Depth' safety philosophy that is insisted upon in UK nuclear plants. The main aim of this philosophy is to avoid situations where an initiating fault can lead directly to an accident with nothing able to prevent it. Although faults cannot be prevented, provisions (engineered systems and/or procedures) can be deliberately put in place to recognise and respond to faults to prevent and/or mitigate the accident that would otherwise ensue (i.e. they provide protection against those faults). Such provisions are known as Safety Systems (SSs)."
4.2 A list of PIEs [Postulated Initiating Events] shall be established to cover all events that could affect the safety of the plant. From this list, a set of design basis events shall be selected with deterministic or probabilistic methods or a combination of both, and used to set the boundary conditions according to which the structures, systems and components important to safety shall be designed, in order to demonstrate that the necessary safety functions are accomplished and the safety objectives met.	4.3 - 2 - i: "In order to assess a plant to the SAP criteria a schedule should be provided that lists all postulated faults and hazards with unacceptable consequences. The schedule should include all initiating faults with their frequencies and consequences, the safety systems and beneficial safety-related systems involved for each initiating fault and the overall protection claim. This is the 'safety schedule' (also known as a fault and protection schedule) - see SAP para 346."
8.3 Only safety systems shall be credited to carry out a safety function.	4.1 - 1 .... There are a number of points to consider which are either implied by or can be deduced from the SAPs' definition *[of a Safety System]*: i) It represents a purely functional definition, there is no implied standard of reliability or robustness. ii) Being a functional definition all aspects of the system that are required to carry out the safety function become encompassed within the definition. These include all elements for a) detecting the fault condition; b) carrying out any decision making processes;

	c) acting to prevent the accident; and d) providing any supporting services which can impair the safety function (i.e. where the system does not fail safe). Procedures such as maintenance, testing and calibration also represent supporting services."
9.1 The fail-safe principle shall be considered in the design of systems and components important to safety.	4.3 - 5 - iii - e: requires "evidence (if claimed) that the system is fail-safe with respect to failure of services and its own predominant failure modes (See Appendix 3 for further information)."
9.2 A failure in a system intended for normal operation shall not affect a safety function.	4.1 - 1 - vi: "SAP ESS19 & associated para 353 do not prohibit other functions being carried out in addition to the fault response function, although singleness-of-purpose is the very strong preference. When additional functions are present it is important to focus on the safety function, and the elements of the overall system that deliver it, and to assess the potential for any of the non-safety functions to interfere with it. The more integrated the non-safety functions, the more likely that their faults will impact on the safety function, and the lower the reliability of the system as a result. The same applies if two or more safety functions are integrated in a single system. Here the same concerns arise with respect to one safety function interfering with another." 4.3 - 5 - iii - b: requires "evidence that the system is independent of and invulnerable to any fault (including any cause of any fault) that it is claimed to act against, and independent of and segregated/separated from all other systems."
9.4 The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components, redundancy, diversity, physical and functional separation and isolation.	4.2 - 6: *[Expectations in terms of reliabilities for different SS configurations]* 4.3 - 4: *[Expectations relating to different configurations of SSs and their implications]* 4.3 - 5: *[Expected features of individual SSs]*
10.2 Instrumentation shall be adequate for measuring plant parameters and shall be environmentally qualified for the plant states concerned.	4.3 - 5 - ii: requires - "d) documentary evidence that the system or its components have been qualified or type tested for worst case environmental conditions. (See also the assessment guides 'Safety Categorisation and Equipment Qualification'[2]' and 'Electromagnetic Compatibility'[5])' e) evidence that the sensors are capable of detecting the condition for which they are claimed, that the detected parameter

	represents as directly as possible the variable of concern rather than implying it indirectly [the point here is that the correlation between the measured value and the value of interest should be rigid and dependable, e.g. if flow detection is required then measurement of dp across an orifice plate is acceptable because the dp/flow correlation is dependable, but measurement of pump speed or pump input power would not be acceptable without specific justification. Calculated parameters may be acceptable, but only if there is no direct means of measurement.], and evidence of life expectancy if they are not replaceable;"
10.7 Redundancy and independence designed into the protection system shall be sufficient at least to ensure that: - no single failure results in loss of protection function; and - the removal from service of any component or channel does not result in loss of the necessary minimum redundancy.	4.3 - 4 - iii: "Where credit is claimed for redundancy or diversity, appropriate levels of separation should be shown between each SS, between the services to each SS (unless the SS is shown to be fail-safe with respect to service failures), and adequate segregation between the SSs and other equipment. Additionally the system as a whole should either be shown to be invulnerable to single failures, or the components with single-failure potential should be shown to be reliable and robust enough for their failure contribution not to compromise system unreliability."
10.8 The design shall permit all aspects of functionality of the protection system, from the sensor to the input signal to the final actuator, to be tested in operation. Exceptions shall be justified.	4.3 - 4 - ii - c: requires information on "the means provided to maintain, calibrate, test (under operational conditions where possible) and inspect each component (including sensors and actuators); the intervals proposed; and the method of reinstatement after maintenance /calibration /testing /inspection. [SSs should be designed and installed so as to facilitate maintenance and testing etc without excessive dose uptake to operators and without introducing new or increased risks.] Proof tests should be shown to be fully effective for *all parts* of the system involved in delivering the relevant safety function, including any automatic testing or diagnostic test equipment used as part of testing, either during service or during proof test. [Ref 12 4.79 et seq. and 4.97 et seq.] The use of bypasses or vetos during proof testing should be minimised and fully justified. If they are to be used, they should be implemented by properly engineered provisions. (See Appendix 2 for further information);"
10.9 The design of the reactor protection system shall minimize the likelihood that operator action could defeat the effectiveness of the protection system in normal operation	4.3 - 5 - ii - f: requires information to be available that either gives or references, for engineered systems, "details of bypasses, vetoes or intended overrides, if any, with

and anticipated operational occurrences.	evidence of necessity, demonstration of sound engineering, means and appropriateness of application and removal, and minimisation of human error potential. (See Appendix 2 for further information.)"
10.10 Computer based systems used in a protection system, shall fulfil the following requirements: - the highest quality of and best practices for hardware and software shall be used; - the whole development process, including control, testing and commissioning of design changes, shall be systematically documented and reviewed; - in order to confirm confidence in the reliability of the computer based systems, an assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken; and - where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.	Appendix 1 - A discussion of problems in dealing with complexity in safety systems (See also T/AST/046 [8] and Ref 12 4.35 and 5.43 et seq.)
Issue K: Maintenance, in-service inspection and functional testing	
2.3 Data on maintenance, testing, surveillance, and inspection of SSCs shall be recorded, stored and analysed. Such records shall be reviewed to look for evidence of incipient and recurring failures, to initiate corrective maintenance and review the preventive maintenance programme accordingly.	4.3 - 11 - ii: "A through life monitoring system should be set up to record all failures and causes of failures affecting safety systems. Such records should be reviewed periodically to allow improvement where possible and update the predictive estimates of hazard frequency and system unavailability in accordance with achieved performance. [Ref 12 6 63 et seq.]"
3.1 SSCs important to safety shall be designed to be tested, maintained, repaired and inspected or monitored periodically in terms of integrity and functional capability over the lifetime of the plant, without undue risk to workers and significant reduction in system availability. Where such provisions cannot be attained, proven alternative or indirect methods shall be specified and adequate safety precautions taken to compensate for potential undiscovered failures.	4.3 - 5 - ii - c: requires information on "the means provided to maintain, calibrate, test (under operational conditions where possible) and inspect each component (including sensors and actuators); the intervals proposed; and the method of reinstatement after maintenance /calibration /testing /inspection. [SSs should be designed and installed so as to facilitate maintenance and testing etc without excessive dose uptake to operators and without introducing new or increased risks.] Proof tests should be shown to be fully effective for *all parts* of the system involved in delivering the relevant safety function, including any automatic testing or

	diagnostic test equipment used as part of testing, either during service or during proof test. [Ref 12 4.79 et seq. and 4.97 et seq.] The use of bypasses or vetos during proof testing should be minimised and fully justified. If they are to be used, they should be implemented by properly engineered provisions. (See Appendix 2 for further information);"

10. REFERENCES

1. HSE, "Safety Assessment Principles for Nuclear Facilities", 2006 Edition (Rev 1), January 2008.

2. Technical Assessment Guide "Safety Categorisation and Equipment Qualification", T/AST/008.

3. Technical Assessment Guides (in preparation) “Human Factors Integration”, T/AST/058 and “Human System Interface and Alarm Handling”, T/AST/059.

4. Technical Assessment Guide "Early Initiation of Safety Systems", T/AST/010.

5. Technical Assessment Guide "Electromagnetic Compatibility", T/AST/015.

6. Technical Assessment Guide "C&I Aspects of Nuclear Plant Commissioning", T/AST/028.

7. Technical Assessment Guide "ONR Guidance on the Demonstration of ALARP (As Low as Reasonably Practicable)", T/AST/005.

8. Technical Assessment Guide "Computer Based Safety Systems", T/AST/046

9. BS IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems, 2002

10. Alarm systems guidance for HID inspectors SPC/TECH/GEN/23, 2003

11. Alarm systems, a guide to design, management and procurement - Engineering Equipment & Materials Users Association Publication No 191, 2007

12. IAEA, Safety Guide - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Standards Series, NS-G-1.3, 2002