Office for Nuclear Regulation

ONR GUIDE			
REDUNDANCY, DIVERSITY, SEGREGATION AND LAYOUT OF MECHANICAL PLANT			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-036 Revision 5		
Date Issued:	April 2017	**Review Date:**	February 2021
Approved by:	G Smith	Mechanical Engineering Professional Lead	
Record Reference:	CM9 Folder 1.1.3.978. (2020/139021)		
Revision commentary:	Rev 4: Routine update Rev 5: Updated review period		

TABLE OF CONTENTS

1. INTRODUCTION

1.1 ONR has established its Safety Assessment Principles (SAPs) [Ref.1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide is one of these guides.

2. PURPOSE AND SCOPE

2.1 This Assessment Guide provides additional information to support the points set out in Health and Safety Executive (HSE) SAPs addressing diversity, redundancy, segregation and layout of mechanical plant. It contains guidance to advise and inform ONR inspectors in the exercise of their professional judgement in reaching regulatory decisions in relation to the assessment of licensees' safety submissions.

2.1 The Guide applies to all measures that contribute to system reliability in the performance of particular safety functions for applications in both nuclear reactors and nuclear chemical plants.

2.3 The Guide is applicable to both new plants, throughout the design, construction and commissioning phases, and to existing operating and decommissioning plants. Because of development in safety standards, existing plant may not comply in every respect with the revised SAPs. Where this is the case ALARP arguments that take account of other factors, such as the age of the plant and projected lifetime, should be considered.

2.4 The Guide does not extend to the detailed design, categorisation, qualification or specification of structures, systems or components (SSCs) particularly in relation to their ability to perform their safety function. What it does consider is the safety duty identified for SSCs in the broad terms of their safety functional requirements, etc.

3 BACKGROUND

Redundancy

3.1 Engineering redundancy is considered to be the provision of more than the minimum number of nominally identical equipment items required to perform a specific safety function. Such redundant provisions allow a safety function to be satisfied when one or more items (but not all) are unavailable, due to a variety of unspecified potential failure mechanisms or maintenance (e.g. identified faults or hazards).

Diversity

3.2 Engineering diversity is considered to be the provision of dissimilar means of achieving the same objective; e.g. the use of features which differ in the physical means of achieving a specific objective or use of different equipment made by different manufacturers.

Segregation

3.3 In a redundant system and despite diverse provisions, the threat of common cause failures from hazards such as fire may be reduced by system segregation. This is the separation of components by distance or physical barriers; an example is the use of fire barriers to mark out individual fire zones, which may also serve as barriers to other hazards.

Layout

3.4 Plant which provides protection against certain faults or hazards should be assessed to ensure that it remains operable and accessible in the event of those faults or hazards occurring. This is particularly important where SSCs important for safety are co-located with other plant which may not be safety related.

4 RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

4.1 Licence Condition (LC) 14: Safety documentation - The licensee shall make and implement adequate arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation.

4.2 Licence Condition (LC) 15: Periodic review - The licensee shall make and implement adequate arrangements for the periodic and systematic review and reassessment of safety cases. It is ONR policy that all safety cases should be reviewed at least every 10 years.

4.3 Licence Condition (LC) 19: Construction and Installation of new Plant - Where the licensee proposes to construct or install any new plant which may affect safety the licensee shall make and implement adequate arrangements to control the construction or installation.

4.4 Licence Condition (LC) 20: Modification of Plant under construction -The licensee shall ensure that no modification to the design which may affect safety is made to any plant during the period of construction except in accordance with adequate arrangements made and implemented by the licensee for that purpose.

4.5 License Condition (LC) 22: Modification or Experiment on existing Plant - The licensee shall make and implement adequate arrangements to control any modification or experiment carried out on any part of the existing plant or processes which may affect safety.

4.6 Licence Condition (LC) 23: Operating Rules - The licensee shall, in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation and to identify the conditions and limits necessary in the interests of safety. Such conditions and limits shall hereinafter be referred to as operating rules.

4.7 Licence Condition (LC) 24: Operating instructions - The licensee shall ensure that all operations which may affect safety are carried out in accordance with written instructions hereinafter referred to as operating instructions.

4.8 Licence Condition (LC) 27: Safety mechanisms, devices and circuits - The licensee shall ensure that a plant is not operated, inspected, maintained or tested unless suitable and sufficient safety mechanisms, devices and circuits are properly connected and in good working order.

4.9 Licence Condition (LC) 28: Examination, inspection, maintenance and testing - The licensee shall make and implement adequate arrangements for the regular and systematic examination, inspection, maintenance and testing of all plant which may affect safety.

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

Relevant SAPs

5.1 The SAPs [Ref.3] directly addressed by this TAG are the following:

- EDR.2 Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.
- EDR.3 Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.
- ELO.1 Access - The design and layout should facilitate access for necessary activities and minimise adverse interactions while not compromising security aspects.
- ELO.2 Unauthorised access to, or interference with, structures, systems and components or their reference data (including Building Information Modelling (BIM)) should be prevented.
- ELO.3 Movement of nuclear matter - Site and facility layouts should minimise the need for movement of nuclear matter.
- ELO.4 Minimisation of the effects of incidents - The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are minimised.
- EMC.29 Redundancy and diversity - Methods of examination of components and structures should be sufficiently redundant and diverse.
- ESS.18 Failure independence - No design basis event should disable a safety system.

5.2 The treatment given to diversity, redundancy, segregation and layout in the SAPs, should not be regarded as necessarily complete. The specific principles are intended to address issues of general significance throughout the nuclear industry, particularly relating to the adequate provision, in relation to safety applications, of:

- Measures to promote robust design
- Pant and equipment layout displaying adequate system functional reliability

5.3 Additional or related issues not directly addressed in the SAPs may be of equal importance in specific circumstances and these aspects of a thorough nuclear safety assessment may need to be identified and considered by the licensee. Such licensee assessments will need to be carefully considered in regulatory assessments.

WENRA Reference Levels

5.4 A review of diversity, redundancy, segregation and layout of mechanical plant against WENRA Reactor Reference Levels [Ref.2] is tabulated in Appendix 1. Other WENRA Reference Levels are not related to the topics in this guide.

IAEA Safety Standards

5.5 The subject of diversity, redundancy, segregation and layout of mechanical plant spans a number of IAEA documents. IAEA documentation that has been drawn upon in the production of this document includes:

- IAEA Safety Standards SSR-2/1 Safety of Nuclear Power Plants: Design. [Ref.3]
- IAEA Safety Guide NS-G-1.10 Design of Reactor Containment Systems for Nuclear Power Plants. [Ref.4]
- IAEA Safety Guide NS-G-1.12 Design of the Reactor Core for Nuclear Power Plants. [Ref.5]
- IAEA Safety Guide NS-G-1.7 Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants. [Ref.6]
- IAEA Safety Guide NS-G-1.9 Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants. [Ref.7]

6 ADVICE TO INSPECTORS

6.1 It is particularly important in nuclear applications to ensure, so far as is reasonably practicable, that safety important equipment will be capable of performing its safety function with an adequate reliability even when the potential for the occurrence of a number of identified faults and/or hazards is significant. This objective may be achieved by the adoption of a number of different plant and equipment provisions, together with the use of techniques to demonstrate the adequacy of the specified measures.

6.2 The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure, and this can be achieved through the consideration of the plant layout. 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.

6.3 In assessing the fitness for purpose of safety important plant, and particularly the ability to perform a primary safety function, a number of issues relating to redundant and diverse provisions need to be considered. Safety cases should identify the safety function of all structures, systems and components (SSCs) so that this assessment can be carried out.

6.4 In achieving the robust design of safety important equipment, which ensures that nuclear plant remains within the specified safety limits, a primary objective is that the chosen systems demonstrate a defence in depth against all identified challenges to the performance of their safety function. Such requirements are closely linked to the system functional reliability and also the ability of a SSC important to safety to perform a safety function in the presence of related SSC failures (reference should be made to ONR guidance relating to probabilistic safety analysis [Ref.8]).

6.5 An assessment of the system reliability, possibly against predetermined target levels, or a separate assessment of the sensitivity of the system to the occurrence of a single

failure, may suggest the provision of more than the minimum number of equipment items to ensure performance of a particular safety function. This feature of engineering design forms a primary means of improving functional performance and reliability, and is frequently referred to as redundancy, a term which implies that the performance of a function does not critically depend on the adequacy of any single provision acting alone.

Redundancy

6.6 A simple check to ensure a minimum level of redundancy is one particular application of the single failure criterion, which tests the ability to perform a safety function in the presence of the single failure of either a passive or an active component in the SSC important to safety.

6.7 Both deterministic and probabilistic arguments should be considered for the provision of redundancy in SSCs. A design which is considered acceptable will display adequate levels of redundancy in plant to ensure that it is fit for purpose and should perform a required safety function. These characteristics will include final provisions which satisfy the deterministic and probabilistic requirements of a potential design of SSCs important to safety.

Diversity

6.8 Where services support plant safety, it should be ensured that the standards applied to this plant are consistent with those applied to the system being supported. This is required so that the fitness for purpose of plant that may be of a lower safety category is unlikely to prevent performance of a safety function by a system of higher safety category. Further information on essential services can be found in ONR guidance relating to essential services [Ref.11].

6.9 Diversity provides one means of protection against some dependent failure mechanisms, by removing common features which may lead to failure dependencies. Diversity particularly provides protection against inherent dependencies and human error related dependencies.

6.10 Diverse provisions should be considered wherever a safety function needs to be satisfied to a reliability that exceeds a limiting value, frequently referred to as the 'common mode' or 'common cause' cut-off value. Typically, this value may be in the range 1.0E-3 to 1.0E-5 failures per demand for nuclear applications. Acceptance of cut-off values lower than 1.0E-5 should be exceptional and will require a very high level of justification (reference should be made to ONR guidance relating to probabilistic safety analysis [Ref.8]).

6.11 The layout and functional design of the nuclear facility and its systems with the possibility of the physical co-location or the functional support of diverse systems leading to dependencies which defeat the objective of providing diversity should be addressed.

Segregation

6.12 Equipment segregation is the separation of redundant and/or diverse components by distance or by barriers to prevent components being damaged, by hazards. Adequate levels of plant segregation should be present in a licensee’s provisions to maximise the likelihood that a safety function will be performed, despite the occurrence of faults and hazards, possibly in combination.

6.13 Segregation is provided in the design to ensure that internal hazards, (e.g. fire and pressure parts failure) and external hazards (e.g. aircraft crash) do not damage separate

trains of safety equipment to the extent that its functional reliability is unacceptably reduced.

6.14 In the event of a hazard, physical segregation typically provides redundancy of active components:

- Quadrant segregation for hot shutdown in the short term
- Half reactor segregation for cold shutdown in the long term

6.15 Segregation can also be provided by distance. This can be achieved by locating redundant (e.g. diesel generators) and diverse (e.g. the essential service water system and reserve ultimate heat sink) equipment in separate buildings.

Layout

6.16 The co-location of redundant systems leading to dependencies might defeat the objective of providing a successful safety function. This should be considered in assessing the layout of nuclear installations and specific systems. The licensee should justify that the fitness for purpose of SSCs important to safety has taken account of the possibility of faults occurring in neighbouring plant and structures, which are not safety related.

6.17 Plant layout should ensure that systems will perform their safety function following any postulated initiating event. Layouts will depend on the specific nuclear installation application and the range of initiating faults considered.

6.18 The plant layout may also affect the extent to which manual intervention requiring local access can be ensured should this be necessary. These aspects of an installation design need to be assessed in relation to the claims made by the licensee regarding access provision during operating and fault conditions.

6.19 Measures should also be taken to ensure unauthorised access to nuclear safety system is prevented. The plant layout may also consider conventional health and safety and human factor challenges for all activities.

Fail-safe design

6.20 Where SSC failure cannot be ruled out on the grounds that its expected frequency is sufficiently low, it may be possible to ensure that in the event of a plant failure the performance of the safety function is unaffected. Where appropriate, plant which fails to operate should fail to a safe condition, not hindering the performance of a safety function. It is important that all identified failure modes are considered.

Essential services

6.21 Services, which are essential to maintain a safe state of the plant may include electricity supplies, cooling water, compressed air or other gases and means of lubrication. Essential services that support equipment forming part of a system important to safety may be regarded as part of the SSC important to safety. Their reliability, redundancy, diversity, independence, provision of features for isolation and for testing of functional capability should be commensurate with the reliability of the system that is supported.

6.22 Where services support plant safety, the standards applied to this plant should be comparable with those applied to the system being supported. This is to ensure that plant of a lower safety category does not prevent performance of a safety function by a system of higher safety category [Ref.11].

Equipment outage

6.23 Where nuclear plant is inoperable at any time, attention should be paid to the effect of its unavailability on the capability to perform essential safety functions and also on its contribution to the risk from the plant. It should be ensured, where practicable, that SSCs important to safety and risk levels are not excessively affected by plant unavailability. Where this cannot be established, specific measures should be defined (e.g. Operating Rules and Instructions) which limit the effect of plant unavailability on the system contribution to the risk.

6.24 In the design of a nuclear installation and SSCs important to safety needed for reliable performance, equipment outages should be taken into account. The impact of the anticipated maintenance, test and repair work on the reliability of each individual SSC important to safety should be included in this consideration. If the resultant reliability or availability to perform a safety function is such that the system no longer meets the criteria used for design and operation, the nuclear plant should be placed in a safe state and the component temporarily out of service should be substituted or restored within a specified time.

Examination, inspection, maintenance and testing (EIMT)

6.25 Provision should be made by the licensee to ensure that the level of plant availability necessary to retain its fitness for purpose is achieved. This is likely to be produced by implementing appropriate maintenance actions, etc. and may be assessed by the effect of such actions on the estimated changes in the contribution to the risk from the plant. Where plant availability is likely to be affected by these maintenance requirements it should be ensured that specified levels of redundancy, diversity and segregation are not compromised. This may involve consideration of the requirements of the plant operating rules, technical specifications and maintenance standards. ONR Guidance on this aspect of functional performance is covered in the TAG on Examination, Inspection, Maintenance and Testing of Items Important to Safety [Ref.12].

6.26 To ensure a high reliability of operation in service SSCs important to safety should be kept in a sound condition by a regular programme of inspection and maintenance; its effectiveness and reliability should be demonstrated by testing, on- or off-load as appropriate; and its availability for operation established by monitoring.

Dependent Failures

6.27 A possible threat to redundant plant is that from dependent failure mechanisms. These have the potential to prevent the performance of a required safety function by simultaneous loss of redundant provisions. Examples of this type of failure are common cause failures (CCF) and the subset of common mode failures (CMF), with plant hazards being a potential initiator of each. The assessor should be satisfied that the risk from dependent failures has been reduced to a level which is acceptable within the limits set by the documented safety case. This should include both deterministic and probabilistic considerations where appropriate.

6.28 A further consequence of the dependent failure mechanism is the limit frequently applied to the reliability benefits claimed from multiple redundancies. System reliability does not generally increase for longer time periods, with increasing levels of redundancy, and this is primarily due to common origin or common cause effects. It should be ensured that excessive benefit is not claimed from multiple redundant systems, and that an appropriate common cause cut-off is applied and justified.

6.29 Where redundant components are provided which satisfy the single failure criterion, and also the reliability requirements, it is necessary for more than one component to fail to

prevent the performance of the system safety function. Increasing the number of redundant components/trains results in a consequential increase in the number of failures required, before the safety function fails to be performed.

6.30 The provision of increasing amounts of redundant equipment does not lead to the reliability of a SSC important to safety increasing indefinitely. The principal reason for an accepted limit to the benefit provided by utilising redundancy in design is the occurrence of failures which have a common origin or other type of common factor. This type of failure is often referred to either as a common cause failure (CCF) or a common mode failure (CMF).

6.31 A CCF is a dependent failure event where approximately simultaneous multiple failures result from a single shared cause (e.g. fire). A CMF is a common cause event where the multiple equipment items fail in the same mode (e.g. failure to reset pumps following maintenance).

6.32 Multiple failures can occur due to common weaknesses or dependencies shared by components. Such failures can cause failure of all redundant components in a single protection system or failure of components in more than one system. Dependent failures can considerably reduce the reliability of the protection systems relative to that expected from consideration of random failure mechanisms acting alone.

6.33 The main types of failure dependencies that can cause potential loss of safety function are:

- **Functional dependencies**, which arise from shared or common functional features; such as a common electrical power source, a common cooling water system or a shared process fluid.
- **Spatial dependencies**, which arise from physical features shared by components located in a common location; such as common radiation or chemical conditions, a common environment and common support structures, and vulnerability to leaks of dangerous fluids (high temperature, corrosive or toxic).
- **Inherent dependencies**, which arise from shared characteristics; such as a common principle of operation or technical embodiment and a common failure mechanism such as mechanical overload or overpressure.
- **Human error related dependencies**, which arise from human errors affecting some shared or common human process; such as human error in design or manufacture, or operating staff error during operation and maintenance.

6.34 To provide protection against dependent failures, one approach, consisting of three main elements, is as follows:

- Failure dependencies are identified and where practicable, measures implemented in design, construction and operation to eliminate the dependencies or reduce their potential effect, examples of such measures are:
    - The provision of segregation to eliminate spatial dependencies; and
    - The avoidance of functional dependencies by segregation of SSCs important to safety and their support services.
- Provide alternative and independent equipment and so eliminate undue reliance on any single system. The purpose of this element of the approach

is to provide protection against any 'hidden failure dependencies' that may not be identified.

- Approaches and procedures should be implemented to minimise the possibility of failure dependencies arising during design, manufacture, construction and operation, including dependencies due to operator and other human error.

6.35 Certain areas in the plant tend to be natural centres of convergence for equipment or wiring of various degrees of importance to safety. Examples of such centres may be containment penetrations, motor control centres, cable spreading rooms, equipment rooms, the control rooms and the plant process computers. Appropriate measures to avoid common cause failures should be provided, as far as reasonably practicable, in such locations where the usual options for defence in depth may not be available.

System Independence

6.36 Systems may be subject to spurious operation in addition to operational failures. These can arise because a given SSC important to safety does not possess a sufficient level of independence from other separate systems. Measures need to be employed by the licensee to ensure that wherever possible a SSC important to safety should not be adversely affected by the spurious operation or failure of other systems, especially through any potential for hidden dependency.

6.37 Actions or inactions, but not necessarily failures resulting from a single mal-operation (failure or spurious action) within one system, may propagate to other systems. This may not be revealed by a conventional dependent failure analysis to address this potential system dependencies can be grouped as system dependency.

6.38 The reliability of systems may be improved by applying the following principles in a structured manor identifying potential system dependency and ensuring system independence in design:

- Maintaining system independence among redundant train components
- Maintaining system independence between train components and the effects of initiating events. For example, an initiating event should not cause the failure or loss of a SSC important to safety or safety function that is required to mitigate that event
- Maintaining appropriate system independence between or among trains, systems or components of different safety categories;
- Maintaining system independence between items important to safety and those not important to safety

6.39 System independence can be achieved by using functional isolation and physical isolation.

Functional Isolation

6.40 Functional isolation should be used to reduce the likelihood of adverse interaction between equipment, components and systems of redundant or connected trains resulting from normal, abnormal or spurious operation, or failure of any component in the trains.

Physical Isolation

6.41 System design utilising the principles of physical isolation should be used as far as reasonably practicable to increase assurance that system independence will be

achieved, particularly in relation to certain common origin events which are not immediately apparent. These principles include:

- Separation by geometry (distance, orientation, etc.)
- Separation by barriers
- Separation by a combination thereof

6.42 The means of separation will depend on the initiating events considered in the design basis. (Reference should be made to ONR guidance relating to deterministic safety analysis and the use of engineering principles in safety assessment [Ref.9]).

Sites with Multiple Units

6.43 For sites with multiple units, e.g. two Reactors, appropriate independence between them should be ensured. The possibility of one unit supporting another unit can be considered provided this is not detrimental to safety.

7 REFERENCES

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

2) WENRA Decommissioning safety reference levels version 2.2 April 2015.

   http://www.wenra.org/media/filer_public/2015/10/14/wgwd_report_decommissioning_srls_v2_2.pdf

3) IAEA Safety Standards: Safety of Nuclear Power Plants: Design SSR-2/1 http://www-pub.iaea.org/MTCD/publications/PDF/Pub1534_web.pdf

4) IAEA – Safety Guide: Design of Reactor Containment Systems for Nuclear Power Plants NS-G-1.10, 2004 http://wwwpub.iaea.org/MTCD/publications/PDF/Pub1189_web.pdf

5) IAEA – Safety Guide: Design of the Reactor Core for Nuclear Power Plants NS-G-1.12 2005. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1221_web.pdf

6) IAEA – Safety Guide: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.7 2004. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1186_web.pdf

7) IAEA Safety Guide: Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, NS-G-1.9 2004. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1187_web.pdf

8) Technical Assessment Guide (Probabilistic Safety Analysis) NS-TAST-GD-030 Rev4 2013 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-030.pdf

9) Technical Assessment Guide (Deterministic Safety Analysis and The use of Engineering Principles in Safety Assessment) NS-TSAT-GD-006 Rev 4 2015 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-006.pdf

10) Technical Assessment Guide (Safety Systems) NS-TAST-GD-003 Rev 7 2014 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-003.pdf

11) Technical Assessment Guide (Essential Services) NS-TSAT-GD-019 Rev 2 2013 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-019.pdf

12) Technical Assessment Guide (Examination, Inspection, Maintenance and Testing of items Important to Safety) NS-TAST-GD-009 Rev 3 Nov 15 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-009.pdf

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

8 GLOSSARY AND ABBREVIATIONS

ALARP	As low as reasonably practicable
CCF	Common Cause Failure
CMF	Common Mode Failure
EDR	Engineering Design for Reliability
ELO	Engineering Layout
EMC	Engineering Integrity of Metal Components and Structures
ESS	Engineering Safety Systems
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
LC	Licence Condition
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation
PWR	Pressurised Water Reactor
SAP	Safety Assessment Principle(s)
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association

A. APPENDICES

APPENDIX 1: COMPARISON WITH WENRA REACTOR REFERENCE LEVELS

A1.1. The following evaluation of WENRA reference levels have been undertaken in respect to diversity, redundancy, segregation and layout of mechanical plant at nuclear installations.

WENRA Reactor Safety Reference Levels	NS-TAST-GD-036: Diversity, Redundancy, Segregation and Layout of Mechanical Plant
Appendix E Design Basis Envelope for Existing Reactors	
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. 9.5 The means for shutting down the reactor shall consist of at least two diverse systems. 9.9 Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of a design basis accident. These lines shall be fitted with at least two containment isolation valves arranged in series. Isolation valves shall be located as close to the containment as is practicable.	The issues of components, redundancy, diversity, physical and functional separation and isolation are addressed in Sections 4.1, 4.2, 4.3, 4.4 and 4.5 with additional information provided in Section 5, Advice to Inspectors.
10.7 Redundancy and independence designed into the protection systems 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.	This issue is addressed in NS-TAST-GD-003 Rev 7 2014, Safety Systems [10].
10.10 Computer based systems used in a protection system, shall fulfil the following requirements: - 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	This issue is addressed in NS-TAST-GD-003 Rev 7 2014, Safety Systems [Ref.10].