|  |
| --- |
|  |
| ONR Technical Assessment Guide  Redundancy, Diversity, Segregation and Layout of Structures, Systems and Components |



ONR Technical Assessment Guide (TAG)

Redundancy, Diversity, Segregation and Layout of Structures, Systems and Components

Authored by: Mechanical Specialist Inspector

Approved by: Mechanical Engineering, Professional Lead

Professional Lead: Professional Lead – Mechanical Engineering Specialism

Issue No.: 6

Publication Date: Nov-23

Next Major Review Date: Oct-28

Doc. Ref.: NS-TAST-GD-036

Record Ref. No.: 2020/139021

Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 4 | Routine update |
| 5 | Updated review period |
| 6 | Major review to body of text. Updated references. Updated to new ONR TAG template |

Contents

[1. Introduction 4](#_Toc146640265)

[2. Purpose and Scope 4](#_Toc146640266)

[3. Background 5](#_Toc146640267)

[4. Relationship to Licence and other Relevant Legislation 8](#_Toc146640268)

[5. Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides 10](#_Toc146640269)

[6. Advice to Inspectors 12](#_Toc146640270)

[References 26](#_Toc146640271)

[Glossary and Abbreviations 29](#_Toc146640272)

[Appendix 1 - Comparison With WENRA Reactor Reference Levels 30](#_Toc146640273)

# Introduction

1. ONR has established its [Safety Assessment Principles](http://www.onr.org.uk/saps/saps2014.pdf) (SAPs) [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 (TAG) is one of these guides.

# Purpose and Scope

1. This technical assessment guide discusses the interpretation of WENRA, IAEA, Relevant Good Practice (RGP) and ONR SAPs [1] to advise and inform ONR inspectors in the exercise of their regulatory judgement.
2. This TAG contains guidance to ONR inspectors in the assessment of licensees’ safety submissions in relation to the redundancy, diversity, segregation and layout of structures, systems and components (SSCs).
3. The TAG applies to SSCs and their function, performance and reliability in supporting safety through redundancy, diversity, segregation and layout in accord with the concepts of common cause failure (CCF) and Defence-In-Depth.
4. The TAG does not extend to the categorisation of SSCs in relation to the ability to perform their designated safety functions. This is further outlined in ONR TAG-094 (Categorisation of Safety Functions and Classification of Structures and Components) [2].
5. The TAG is applicable to:

* new facilities throughout the design, construction, and commissioning phases; and
* operating facilities, throughout use into post-operational care & maintenance, and eventual decommissioning.

1. Due to the ongoing development of safety standards, aging facilities may not comply in every respect with the revised ONR SAPs [1]. Where this is the case; inspectors should use their judgement and discretion in the depth and scope in which they utilise this guidance.

# Background

1. For the purposes of this TAG, the following definitions apply:

## Redundancy

1. Redundancy is the provision of alternative (identical or diverse) structures, systems, or components, so that any single structure, system, or component can perform the required function regardless of the state of operation, or failure, of any other [1].
2. Redundant provisions allow a safety function to be satisfied when one or more items (but not all) are unavailable, due to maintenance activities or potential failure mechanisms (e.g. identified faults or hazards).

## Diversity

1. Diversity is defined as the presence of two or more systems or components to perform an identical function, where the different systems or components have different attributes so as to reduce the possibility of CCF, including Common Mode Failure (CMF). [1]

* CCF is the failure of two or more SSCs in the same manner or mode due to a single specific event or cause.
* CMF is a type of CCF, in which the SSCs fail in the same way (although they may not be in close proximity).

## Segregation

1. Segregation is the physical separation of SSCs by distance or by means of some form of barrier that reduces the likelihood of CCF. For example: The use of fire barriers between diesel generators to create individual fire zones, which may also serve as barriers to other hazards (such as projectiles).

## Layout

1. The design and layout of the site, its facilities (including enclosed facilities), support facilitates, and services should be such that the effects of faults and accidents are minimised (ONR SAP ELO.4) [1]
2. Plant layout should reflect established good practice, and facilitate access for necessary operational and maintenance activities (personnel and equipment access, laydown areas etc.).
3. Attention should be given to the layout of plant where safety related SSCs are co-located with other systems, to ensure that the area remains accessible in the event of a hazard or fault condition.
4. A Failure is a loss of the ability of a structure, system or component to function within acceptance criteria. Note that the SSC is considered to fail when it becomes incapable of functioning, whether or not it is required at that time.

## Defence-In-Depth

1. Defence-In-Depth is covered in detail in NS-TAST-GD-051 ‘The Purpose, Scope, and Content of Safety Cases’ [3] but is included at high level here for completeness.
2. ‘Defence-In-Depth’ is a hierarchical deployment of differing levels of diverse equipment and procedures which aims to:

* prevent faults arising;
* provide protection in the event that prevention fails; and
* provide mitigation should an incident occur.

1. The SAPs expect that the safety case demonstrates Defence-In-Depth (SAP EKP.3) [1]. Defence-In-Depth is generally applied in five levels which should be, as far as practicable, independent from one another.
2. The methodology should ensure that if one level fails, it will be compensated for, or corrected by, the subsequent level.
3. When properly implemented, Defence-In-Depth ensures that no single:

* human-induced event;
* organizational shortcoming; or
* technical failure;

could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability.

1. The independent effectiveness of the different levels of defence is a necessary element of Defence-In-Depth. Table 1 below and outlines the five levels of defence in depth. For further information, refer to ONR SAPs [1] and TAGs.

Table 1 - Objectives of the levels of protection

|  |  |
| --- | --- |
| Level | Objective |
| Level 1 | Prevention of abnormal operation and failure by design. |
| Level 2 | Prevention and control of abnormal operation and detection of failures. |
| Level 3 | Control of faults within the design basis to protect against escalation to an accident. |
| Level 4 | Control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents. |
| Level 5 | Mitigation of radiological consequences of significant release of radioactive material. |

1. The IAEA Fundamental Safety Principles (para. 3.31) [4] state that “Defence-In-Depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment.”

# Relationship to Licence and other Relevant Legislation

## LICENCE CONDITONS:

1. The Nuclear Site Licence Conditions place legal requirements on the licensee to make and implement arrangements to ensure that safety is being managed adequately. When considering compliance with the following licence conditions, consideration should be given to good practices for redundancy, diversity, and segregation. Ageing facilities and sites undergoing decommissioning may not fully comply to the updated SAPs and will be require an adequate ALARP justification.

* 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.
* 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.
* 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.
* 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.
* 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.
* 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.
* 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.
* 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.
* 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.

## OTHER RELEVANT LEGISLATION

1. The principles of redundancy, diversity, segregation and layout are not exclusive to nuclear safety and are equally appliable to conventional health and safety. The following is a non-exhaustive list of relevant legislation:

* Control of Major Accident Hazards Regulations (COMAH) 2015.
* Dangerous Substances and Explosive Atmospheres Regulations (DSEAR) 2002.

## APPROVED CODES OF PRACTICE

1. The following is a non-exhaustive list of approved codes of practice making reference to either redundancy, diversity, segregation or layout:

* Dangerous Substances and Explosive Atmospheres – Approved Code of Practice and Guidance: L138 (2nd Edition), 2013.

# Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides

## WENRA Reference Levels

1. A review of diversity, redundancy, segregation, and layout of facilities against WENRA Reactor Reference Levels [5] is tabulated in Appendix 1. Other WENRA Reference Levels are not related to the topics in this TAG.

## IAEA Safety Standards

1. The subject of redundancy, diversity, segregation, and layout spans a number of IAEA documents. IAEA documentation that has been referenced in the production of this document includes:

* IAEA Specific Safety Standards SSR-2/1(Rev.1): Safety of Nuclear Power Plants: Design. [6]
  + Req. 21 – Physical Separation and Independence of Safety systems
  + Req. 24 – Common Cause Failures
* IAEA Specific Safety Guide.39: Design of Instrumentation & Control Systems for Nuclear Power Plants [7]
  + Para 6.20 – I&C systems should be redundant to the degree necessary to meet the requirements for I&C reliability and the single failure criterion.
  + Para 6.61 – Where diversity is provided, it should be demonstrated that the choice of the types of diversity used achieves the common cause mitigation that is claimed.
* IAEA Specific Safety Guide SSG.53: Design of Reactor Containment and Associated Systems for Nuclear Power Plants. [8]
  + Para 3.11(b) – Layout, Redundancy, and Segregation
  + Para 3.55 – Identify common cause failures between redundancies and implement provisions to ensure independence so far as is reasonably practicable (SFAIRP) (See also: ONR-GEN-GD-018 [9])
  + Para 3.58 – Common cause failures, initiating events and design basis and limits
* IAEA Safety Guide SSG-52: Design of the Reactor Core for Nuclear Power Plants. [10]
* IAEA Safety Guide NS-G-1.7: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants. [11]
* IAEA Safety Guide SSG-56: Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants. [12]
* INSAG-10 – Defence in depth in nuclear safety [13]

# Advice to Inspectors

1. The UK nuclear safety regime features Defence-In-Depth concepts which were developed from the military when establishing multiple barriers to attack. The concept of providing multiple barriers (and protection to prevent breach of these barriers) is an established part of UK nuclear safety goal-setting regime. It compensates for uncertainty caused by equipment failure and human error.
2. Despite apparent robustness, a barrier can still fail. This is why the concepts of redundancy, diversity, segregation and layout are needed to provide ‘additional’ barriers or ‘Defence-In-Depth’.
3. ONR’s SAPs [1] set-out ONR’s expectations for Defence-In-Depth. Facilities should be designed and operated so that Defence-In-Depth against potentially significant faults is achieved by provision of multiple independent barriers to fault progression.
4. ONR expects licensees to take a proportionate approach to demonstrating Defence-In-Depth, as part of a nuclear safety case. The starting point is a thorough and systematic hazard and fault identification, leading to a demonstration that the design conforms to good engineering practice and sound safety principles. This is followed by the analysis of faults using complimentary techniques of:

* Design Basis Analysis (DBA);
* Probabilistic Safety Analysis (PSA); and / or
* Severe Accident Analysis (SAA) – if necessary.

1. The application of deterministic safety principles requires licensees to ensure effective application of DBA which will ensure that the design has robust protection, even when making conservative assumptions for normal operations and allowances for single failures.
2. The principal aim of a DBA is the robust demonstration of the fault tolerance of the system or facility, including the effectiveness of its safety measures. The DBA will guide the design requirements, including modifications, to determine the limits to safe operation and deliver safety functions reliably during all modes of operation.
3. ONR expects licensees to design for reliability. The key principles of design will feature:

* Redundancy to avoid the effects of random failure;
* Diversity and Segregation to avoid the effects of CCF; and
* Single Failure Tolerance.

1. For nuclear applications it is important to ensure, so far as is reasonably practicable, that equipment important to safety will be capable of performing its safety function with adequate reliability, even when the potential occurrence of identified faults and/or hazards is significant. This objective can be achieved by the adoption of plant and equipment provisions, together with the use of techniques to demonstrate the adequacy of the specified measures.
2. The plant should incorporate redundancy, diversity, and segregation of SSCs to avoid the effects of random, and CCF. This can be achieved through consideration of the regulatory expectations contained below for each of the requirements for redundancy, diversity and segregation.
3. In assessing whether equipment important to safety is fit for purpose, and its ability to perform its primary safety function; issues relating to the provision of redundancy, diversity and segregation should be considered. The duty holder’s safety case should seek to identify the safety function of all relevant SSCs with the safety assessment setting out how Defence-In-Depth is achieved through design.
4. A primary objective to demonstrate the robust design of safety related SSCs is the demonstration of Defence-In-Depth against all identified fault conditions in relation to the performance of their safety function. This requirement is closely linked to the system functional reliability, in the presence of related SSC failures.
5. An assessment of system reliability against predetermined targets (or the sensitivity of the system to the occurrence of a single failure) may indicate a need for multiple SSCs required to ensure the performance of a particular safety function through redundancy, diversity, segregation and layout.
6. The concepts outlined below are to aid inspectors in assessing the adequacy of the claimed levels of redundancy, diversity, or segregation. This guidance is targeted towards:

* new facilities throughout the design, construction, and commissioning phases; and
* operating facilities, throughout use into post-operational care & maintenance, and eventual decommissioning.

## REDUNDANCY

1. A single SSC should not be capable of simultaneously affecting redundant parts of a safety system and compromising the capability of associated SSCs to perform their safety functions.
2. An acceptable minimum level of redundancy can be determined from the analysis of the ‘Single Failure Tolerance’; an analysis assumption that considered the SSCs ability to perform a safety function in the presence of a single failure event in the SSC train.
3. Further information is available in TAG-006 – Design Basis Analysis [14]
4. ONR SAPs (Para. 183) [1] state it should be demonstrated that the required level of reliability for [the SSCs] safety function can be achieved.
5. An adequate demonstration of redundancy cannot be claimed solely from the provision of multiple lines of identical SSCs. For example, a system of two-parallel trains of pressure-relief valves might be claimed to reduce the probability of failure due to redundant valves. However, increasing the number of valves increases risk of spurious opening, resulting in an undesirable plant configuration. Therefore; redundancy in combination with diversity (different valve types and operating conditions) can reduce the risk of CCF.
6. If a demonstration of redundancy is not feasible (i.e. during the Generic Design Approval (GDA) process), both deterministic and probabilistic arguments should be considered to demonstrate that the required level of reliability for the SSCs intended safety function can be achieved.
7. Further examples that demonstrate how redundancy of SSCs can be applied in practice include:

* Defence-In-Depth: The provision of additional measures to prevent sever accidents can be satisfied by the use of multiple emergency diesel generators, to act as back-up in case a fault-scenario prevents the primary system from achieving its classified safety function.
* In ageing facilities, redundancy and diversity requirements can be satisfied simultaneously by retrofitting SSCs that mitigate the loss of a safety function. An example of this would be the retrofitting of an uninterruptible power supply for ventilation extract fans to protect against a loss of power.
* ‘Design for Reliability’ as demonstrated in Advanced Gas-cooled Reactors (AGRs) which use Gas Circulators (GC) to aid reactor cooling. In the event of the GCs becoming unavailable, AGR cooling can be provided by design though natural thermal convection of the coolant.

### DEPENDENT FAILURES

1. A ‘Dependent Failure’ is defined in the ONR SAPs [1] as a failure of two or more SSCs occurring due to a single specific event or cause. Dependent failure mechanisms have the potential to prevent the system performing its required safety function due to a simultaneous loss of redundant provisions. Examples of dependent failure mechanisms are CCF and CMF.
2. A CCF is a type of dependent failure where 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).
3. ONR SAPs [1] (EDR.3) state that CCF should be addressed explicitly where an SSC employs redundant or diverse components, measurements, or actions to provide high reliability.
4. The assessor should be satisfied that the risk from dependent failures has been reduced ALARP and within the limits defined by the safety case. This should include both deterministic and probabilistic considerations, where appropriate.
5. IAEA SSR 2-1 [6] states “The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability”.
6. A consequence of the dependent failure mechanism is to limit the reliability benefits claimed from several lines of defence (multi layered redundancies). System reliability does not generally increase with time, or with increasing levels of redundancy, primarily due to common origin or common cause effects. Therefore, the provision of increasing amounts of redundancy does not lead to the reliability claim for SSCs increasing indefinitely.
7. Where redundant components are provided the design should ensure that more than one component must fail to disrupt the system safety function. Increasing the number of redundant SSCs results in a consequential increase in the number of failures required to impact the system safety function. However, it’s important that unrealistic reliability is not claimed from multiple redundant systems recognising an appropriate common cause cut-off should be applied and justified.
8. Multiple failures can occur due to common weaknesses or dependencies shared by components. Such failures can impact all redundant components in a single protection system or lead to the failure of components in more than one system. Dependent failures can reduce the reliability of the protection systems similar to random failure mechanisms acting alone.
9. The main types of failure dependencies that can cause potential loss of safety function are:

* **Functional dependencies,** arising 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**, arising 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.

1. An approach to provide protection against dependent failures is as follows:

* Identify, and where practicable, implement measures in design, construction, and operation to eliminate the dependencies or reduce their potential effect. For Example:
  + Segregate SSCs to eliminate spatial dependencies; and
  + Segregate SSCs and their support services to avoid functional dependencies.
* Provide alternative and independent equipment to eliminate undue reliance on any single system. The purpose of this approach is to provide protection against any failure dependencies that may not be identified.
* Minimise the possibility of failure dependencies arising during design, manufacture, construction, and operation. For example: minimising dependencies due to operator and other human error.

1. Centres of convergence for equipment, cables or pipework can occur in containment penetrations, motor control centres, cable spreading rooms, equipment rooms, the control rooms, and the plant process computers. Appropriate measures to avoid CCF’s should be provided, as far as reasonably practicable, in such locations where the usual options for Defence-In-Depth may not be available.
2. Practical examples of dependant and CCF include the following:

* The incident at Fukushima in 2011 is a key example of a single event causing widescale disruption to all safety systems, regardless of diversity, layout or segregation. This event highlights the requirement for safety systems to be tolerant to CCF’s, and the need for all safety systems not to rely on common electrical power, or other single driving mechanism.
* Indirect CCF from inadequate EIMT arrangements can impact multiple systems across multiple sites. A large number of safety systems at a generating site were affected by a high level of corrosion, including a number of systems corroded to a level where there was debate about their ability to perform their safety function, if required.

## DIVERSITY

1. Diversity provides a means of protection against some dependent-failure mechanisms by removing common features which may result in CCF.
2. Diversity can be demonstrated in many ways, including:

* Human diversity
* Design diversity
* Software diversity
* Functional diversity
* Signal diversity
* Engineered diversity

1. Engineering Diversity can provide Defence-In-Depth against inherent failure dependencies and human-error related failure dependencies. This can be further defined as:

* **Conceptual Diversity:** Different design philosophies (Control rods Vs Boronated water injection).
* **Functional Diversity:** Equipment that is functionally diverse (Volumetric pump Vs Centrifugal pumps).
* **Manufactured Diversity:** Different component suppliers.

1. For further information, please refer to NUREG CR/6303 - Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems [15]
2. Where services support plant safety, a consistent approach is required when selecting standards applicable to both the plant, and the system being supported. However, services that are required for the safety system to deliver a given safety function should be classified at the same level as the safety system. Further information on essential services can be found in ONR TAG-019 (Essential Services) [16]
3. Diverse provisions, the provision of more than one diverse system / train, should be considered wherever a safety function needs to be satisfied to a reliability that exceeds a limiting value (the 'common mode' or 'common cause' cut-off value. Note: the cut-off value is the maximum reliability that can be claimed for a single system regardless of its diversity or redundancy). Typically, this value ranges from 1x10-3/year to 1x10-5/year failures per demand for nuclear applications.
4. Acceptance of cut-off values lower than 1x10-5/year should be exceptional and will require a very high level of justification. Generally, the requirement for frequent faults >1x10-3/year is at least two diverse systems / trains. The deterministic approach to diversity analyses should be completed by a probabilistic assessment of the design. This is further explained in ONR TAG-006 (Design Basis Analysis) [14] and TAG-030 (Probabilistic Safety Analysis) [17].
5. The Duty Holder must be able to demonstrate that a structured approach has been taken to evaluate the CCF risk associated with each type of SSC that may be used in both First Line SSCs, and Diverse Line SSCs.
6. A graded approach, defined by an SSCs ability to fulfil the safety function, is generally acceptable. The goal is for the duty holder to demonstrate that CCFs cannot prevent a diverse train of SSCs fulfilling their safety functions.
7. Adequate demonstrations of diversity can be a challenge for nuclear new builds when considering inter-linked global supply chains. Based on the output from the safety case deterministic study, the diversity design requirements at the component level can be defined before engaging with the supply chain.
8. It is important that safety related SSCs and sub-components are shown not to be sourced from the same sub-supplier / contractor, where reasonably practicable. The licensee should be able to demonstrate that supply chain management, organisation, and processes ensure that design diversity requirements are not challenged when sourcing items and equipment.
9. Practical Examples of diversity by design include:

* Fuelling machines which use safety system voting logic to ensure next step in the process is safe to carry out. Positive confirmation that valves have been closed, pressure boundary components extended, correct pressures achieved need to be confirmed before next step in process can be carried out. This highlighting redundancy in the system along with diversity given different instrument types used and protection against CCF.
* Nuclear lifting assemblies typically rely on a level of redundancy and diversity in the design that goes beyond a “one fail-safe” approach, which allows for an independently operable load path the capability to support the load. These redundant or diverse systems must be designed such that they are capable of sustaining the maximum dynamic load resulting from the failure of the primary system [18].
* Operational Diversity as demonstrated by the HPR1000 Isolation Dampers, which feature an automated control function while retaining the ability to be ‘manually triggered’ from the main control room.

## SEGREGATION

1. Equipment segregation is the separation of diverse and/or redundant components by distance, or physical barriers, to reduce the risk of safety related SSCs being damaged by local hazards or interference between SSCs (for example disintegration of one SSC could impact an adjacent SSC).
2. Adequate levels of plant segregation should be present in a licensee’s provisions to maximise the likelihood that a safety function can be achieved, despite the occurrence of faults and hazards, possibly in combination.
3. IAEA SSR2-1 Requirement 21 [6] states: “Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence, and independence of communication (data transfer), as appropriate”.
4. Segregation should be evident in the plant design to ensure that internal hazards, (e.g. fire and pressure-systems failures) and external hazards (e.g. aircraft impact) do not damage separate trains of safety equipment to the extent that its functional reliability is unacceptably reduced.
5. IAEA SSG-53 [8] states “The redundancies of the systems should be segregated to the extent possible, or adequately separated, and should be protected as necessary to prevent the loss of the safety function performed by the system”.
6. In the event of a hazard, physical segregation typically ensures that redundancy of active components is protected. For example:

* Quadrant segregation for reactor hot shutdown
* Half reactor segregation for cold shutdown
* Full segregation for fire or projectile protection (The application of segregation and layout of Sizewell B’s emergency diesel generators)

1. 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.
2. Practical examples of segregation by design include:

* Nuclear Power plants featuring multiple segregated emergency control rooms
* Multiple EIMT teams responsible for segregated systems; such as multiple teams conducting EIMT operations on a PWR cooling loop
* On-site and off-site emergency diesel generator units
* Ventilation systems should demonstrate the segregation of essential services (e.g. electrical supplies) to ensure defence-in-depth against CCF and CMF (e.g. fire)

## LAYOUT

1. Consideration should be given to the layout, and physical co-location of safety related SSCs for normal operation, fault condition, and EIMT activities. ONR SAPs [1] ELO.4 states 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.
2. In justifying that the SSCs important to safety are fit for purpose, the licensee should identify faults in neighbouring plant and confirm there is no direct impact on the SSCs safety function, so far as reasonably practicable.
3. Plant layout should ensure that systems will perform their safety function following any postulated initiating event. Plant layout will depend on the specific nuclear installation application and the range of initiating faults considered.
4. Local access to equipment (for EIMT or manual intervention) is defined by the plant layout. The design and installation of SSCs should be addressed with regards to access provision claims made by the duty holder during both operating, and fault conditions. The plant layout may also consider conventional health and safety and human factor challenges for all activities.
5. For conventional health and safety considerations, the assessor should be aware of ‘The Dangerous Substances and Explosive Atmospheres Regulations’ (DSEAR) [19] and its requirements. (For example; Section 2 states that the workplace should be “designed, constructed and maintained so as to reduce risk”.)
6. DSEAR puts duties on employers to protect people from these risks to their safety in the workplace, and to members of the public who may be put at risk by work activity. Therefore, it may be required to undertake or commission a DSEAR risk assessment to fully understand the risks present. More information can be found in ACoP L134: ‘Design of Plant, Equipment and Workplaces.’
7. Measures should also be taken to prevent unauthorised access to nuclear safety systems, as outlined in ONR SAPs [1] (ELO.2) “Unauthorised access to, or interference with, structures, systems and components or their reference data (including Building Information Modelling (BIM)) should be prevented”.
8. There are 4 key considerations that support Layout:

System Independence

1. IAEA SSR-2/1 states [6] a requirement for the physical separation and independence of safety systems. This can be demonstrated via the independence implemented between instrumentation and control systems, or in the support systems necessary for the actuation and operation of the instrumentation and control systems, which should not be compromised by CCF.
2. Systems may be subject to spurious operation, in addition to operational failures, which may arise due to SSCs important to safety not possessing an adequate level of independence from other safety systems. Duty holders should ensure that, so far as is reasonably practicable, an SSC important to safety is not adversely affected by the spurious operation or random failure of associated or adjacent systems, especially through any potential for hidden dependencies.
3. Adverse effects resulting from mal-operation (but not necessarily failures) within a system may propagate to other systems through system-based dependencies. These system dependencies may not be evident through a conventional dependent failure analysis.
4. The reliability of systems can be improved by identifying potential system dependencies and ensuring system independence from the design stage, with a structured approach to the following:

* 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 an SSC important to safety, or the safety function that is required to mitigate that event);
* Maintaining an appropriate level of system independence between trains, systems, or components of different safety categories;
* Maintaining system independence between items important to safety and those not important to safety.

1. System independence can be achieved by demonstrating functional isolation and physical isolation of critical SSCs. ONR SAPs [1] (ESS.18) state that no design basis event should disable a safety system.

Functional Isolation

1. Functional isolation should be utilised 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

1. Systems designed utilising the principles of ‘physical isolation’ should be implemented as far as reasonably practicable to increase assurance that system independence will be achieved, particularly in relation to CCF events which are not immediately apparent.

* Principles of physical isolation include:
* Separation by geometry (distance, orientation, etc.);
* Separation by suitable barriers (Firewalls); and
* Separation by a combination of the above.

1. The method of physical isolation will depend on the initiating events considered in the design basis. More information is provided in the ONR SAPs [1] relating to the use of engineering principles in safety assessments.

Sites with Multiple Units

1. 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. This is reflected in modern design principles supporting GDA activities. For decommissioning sites, a practical example of good plant layout can be demonstrated through waste package segregation by activity levels.

## OTHERS MATTERS FOR INSPECTOR CONSIDERATION

### FAIL SAFE DESIGN

1. Where appropriate, SSCs should be designed to a ‘fail-safe’ condition, not hindering the performance of a safety function. If SSC failure cannot be excluded on the sole basis that the expected failure frequency is sufficiently low, it should be demonstrated that in the event of a plant failure, the performance of the safety function is unaffected. It is important that all identified failure modes are considered SFAIRP.

### EXAMINATION, INSPECTION, MAINTENANCE, AND TESTING (EIMT)

1. Provision should be made for a minimum level of plant to be available during EIMT activities to retain the plants safety function. This can be achieved by implementing appropriate maintenance regimes, the effectiveness of which can be assessed by changes in risk from the remaining operational plant. Consideration should be given to the use of diverse maintenance teams with suitable approvals to prevent errors leading to CCF’s.
2. To ensure a high reliability of operation in service, SSCs important to safety should be kept in an acceptable condition through a regular programme of inspection and maintenance; the effectiveness and reliability of the EIMT arrangements should be demonstrated by testing and its availability for operation established by monitoring.
3. It should be ensured that plant availability, including levels of redundancy, diversity, and segregation, are not compromised during routine maintenance activities. This may involve consideration of the requirements of the plant operating rules, technical specifications, and maintenance standards. Further information can be found in ONR TAG 009 – Examination, Inspection, Maintenance and Testing of Items Important to Safety [20].

### EQUIPMENT OUTAGE

1. Where nuclear plant is unavailable at any time, attention should be given to the effects on the remaining plant capability to perform essential safety functions, and the contribution to the overall risk from the unavailable plant. It should be ensured, where practicable, that risk levels and SSCs important to safety and are not adversely affected by plant unavailability. Where this cannot be guaranteed, specific measures should be defined which limit the effect of plant unavailability on the system contribution to the risk. Guidance on operating instructions can be found in ONR Technical Inspection Guide (TIG) 024 – Operating Instructions [21].
2. In the design of nuclear installations and SSCs required for safe and reliable performance, planned equipment outages should be considered. The impact of the EIMT work on the reliability of each individual SSC important to safety should be included in these considerations. If the resultant reliability, or availability to perform a safety function, no longer meets the criteria used for design and operation, the nuclear plant should be placed in a safe state, and the SSC temporarily out of service should be substituted or restored within a suitable period.

### ESSENTIAL SERVICES

1. Services which are essential to maintain the safe state of the plant may include:

* Electricity supplies;
* Cooling water;
* Compressed air or other gases (Nitrogen); and
* Means of lubrication.

1. Essential services that support SSCs important to safety, may be regarded as part of that SSC. The reliability diversity, redundancy, segregation, and provision of features for isolation and testing of functional capability should be commensurate with the reliability of the system being supported.
2. Where services support plant safety, a consistent approach to the selection of standards applied to both the plant, and the support system is required. It is unlikely that a plant with a lower safety function category will reduce the performance of a safety function by a plant or system with a higher safety function category. However, services that are required for the safety system to deliver a given safety function should be classified at the same level as the safety system (SAPs ECS.2) [1]. Further information on essential services can be found in TAG-019 (Essential Services) [16].

### CONSTRUCTION DESIGN & MANAGEMENT REGULATIONS 2015

1. The Construction (Design and Management) Regulations 2015 (CDM 2015 [22]) is the main set of regulations for managing the health, safety, and welfare of construction projects in Great Britain (GB). CDM 2015 is a relevant statutory provision (RSP) made under the Health and Safety at Work etc. Act 1974 (HSWA74), which ONR enforces on GB nuclear sites, authorised defence sites, and new nuclear build sites.
2. All ONR regulated sites carry out work that falls under the scope of CDM 2015 throughout its life cycle, from design concept to decommissioning and demolition. The scope of the CDM regulations are wide-ranging and apply to all construction work throughout the entirety of the construction process, including:

* design;
* new build;
* demolition;
* modifications;
* refurbishments;
* repair; and
* maintenance of a building and/or a civil structure.

1. In addition, consideration should be given to any foreseeable hazards to the facility, its structures, systems or components that originate within the site boundary, and over which the duty-holder has some control (I.E. Identified internal hazards)
2. Further information regarding the CDM regulations can be found in NS-INSP-GD-074 ‘Construction (Design and Management) Regulations 2015’ [23] and NS-TAST-GD-014 ‘Internal Hazards’ [24].

# References

|  |  |
| --- | --- |
| [1] | ONR, *Safety Assessment Principles for Nuclear Facilities. 2014 Edition.,* http://www.onr.org.uk/saps/saps2014.pdf, Revision 1 (January 2020). |
| [2] | ONR, *NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures and Components,* http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-094.pdf, (July 2019). |
| [3] | ONR, *NS-TAST-GD-051 - The purpose Scope and Content of Nucelar Safety Cases,* http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-019.pdf , Rev 8 (December 2019). |
| [4] | IAEA, *Fundamental Safety Principles - No.SF-1,* https://www.iaea.org/publications/7592/fundamental-safety-principles, 2006. |
| [5] | WENRA, *Decommissioning safety reference levels,* http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf, Version 2.2 (April 2015). |
| [6] | IAEA, *SSR-2/1 (Rev 1.) Safety of Nuclear Power Plants: Design,* http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf, (2016). |
| [7] | IAEA, *SSG-39: Design of instrumentation and Control Systems for Nuclear Power Plants,* https://www-pub.iaea.org/MTCD/publications/PDF/Pub1694\_web.pdf, 2016. |
| [8] | IAEA, *SSG-53 - Design of Reactor Containment Systems for Nuclear Power Plants,* http://www-pub.iaea.org/MTCD/Publications/PDF/P1856\_web.pdf, (2019). |
| [9] | ONR, *ONR-GEN-GD-018 - So Far As Is Reasonably Practicable (SFAIRP),* Rev 0. (2019). |
| [10] | IAEA, *SSG-52 - Design of the Reactor Core for Nuclear Power Plants,* http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1859\_web.pdf, (2019). |
| [11] | IAEA, *NS-G-1.7 - Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants,* http://www-pub.iaea.org/MTCD/publications/PDF/Pub1186\_web.pdf, (2004). |
| [12] | IAEA, *SSG-56 - Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants,* http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1878\_web.pdf, (2020). |
| [13] | IAEA, *INSAG-10: Defence in Depth in Nuclear Safety,* https://www-pub.iaea.org/mtcd/publications/pdf/pub1013e\_web.pdf, 1996. |
| [14] | ONR, *NS-TAST-GD-006 - Design Basis Analysis,* https://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-006.docx. |
| [15] | N. R. Commission, *NUREG CR/6303 - Method for Performing Diversity and Defence in Depth Analyses of Reactor Protection Systems,* https://www.nrc.gov/docs/ML0717/ML071790509.pdf, 1994. |
| [16] | ONR, *NS-TAST-GS-019 - Essential Services,* http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-019.pdf, Rev 5 (July 2019). |
| [17] | ONR, *NS-TAST-GD-030 - Probabilistic Safety Analysis,* http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-030.pdf, Rev 7 (June 2019) . |
| [18] | ONR, *NS-TAST-GD-056 - Nuclear Lifting Operations,* http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-056.pdf, Rev 7. (October 2018). |
| [19] | HSE, *The Dangerous Substances and Explosive Atmospheres Regulations,* https://www.hse.gov.uk/fireandexplosion/dsear.htm, (2002). |
| [20] | ONR, *NS-TAST-GD-009 - Examination, Inspection, Maintenance and Testing of items Important to Safety,* http://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-009.pdf, Rev 5 (May 2019). |
| [21] | ONR, *NS-INSP-GD-024 - LC24 Operating Instructions,* http://www.onr.org.uk/operational/tech\_insp\_guides/ns-insp-gd-024.pdf, Rev 6 (Septemer 2019). |
| [22] | HSE, *The Construction (Design and Management) Regulations,* https://www.hse.gov.uk/construction/cdm/2015/index.htm, (2015). |
| [23] | ONR, *NS-INSP-GD-074 - Construction (Design and Management) Regulations 2015,* https://www.onr.org.uk/operational/tech\_insp\_guides/ns-insp-gd-074.pdf , Rev 0 (October 2021). |
| [24] | ONR, *NS-TAST-GD-014 - Internal Hazards,* https://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-014.pdf , Rev 7 (October 2021). |
| [25] | ONR, *NS-TAST-GD-003 - Safety Systems,* https://www.onr.org.uk/operational/tech\_asst\_guides/ns-tast-gd-003.docx. |

# Glossary and Abbreviations

AGR Advanced Gas cooled Reactor

ALARP As low as reasonably practicable

BIM Building Information Modelling

CCF Common Cause Failure

COMAH Control of Major Accident Hazards Regulations

CMF Common Mode Failure

DBA Design Basis Analysis

ECS Engineering Safety Classification and Standards

EDR Engineering Design for Reliability

EIMT Examination, Inspection, Maintenance and Testing

ELO Engineering Layout

EMC Engineering Integrity of Metal Components and Structures

ESS Engineering Safety Systems

GDA Generic Design Assessment

GC Gas Circulator

HSE Health and Safety Executive

HSWA74 The Health and Safety at Work etc Act 1974

IAEA International Atomic Energy Agency

LC Licence Condition

LOLER Lifting Operations and Lifting Equipment Regulations

ONR Office for Nuclear Regulation

PSA Probabilistic Safety Analysis

PSSR Pressure Systems Safety Regulations

RGP Relevant Good Practice

RPV Reactor Pressure Vessel

SAA Severe Accident Analysis

SAP Safety Assessment Principle(s)

SFAIRP So Far As Is Reasonably Practicable

SRV Safety Relief Valve

SSCs Structures, Systems and Components

TAG Technical Assessment Guide(s)

TIG Technical Inspection Guide(s)

WENRA Western European Nuclear Regulators’ Association

# Appendix 1 - Comparison With WENRA Reactor Reference Levels

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

| **WENRA Reactor Safety Reference Levels** | **NS-TAST-GD-036: Diversity, Redundancy, Segregation and Layout of 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 5.1, 5.2, 5.3, 5.4 and 5.5 with additional information provided in Section 6, [Advice to Inspectors.](#advice) |
| 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 [25] |
| 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 9 2018, Safety Systems [25]. |