ONR GUIDE			
Essential Services			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-019 Revision 5		
Date Issued:	July 2019	**Review Date:**	April 2024
Approved by:	Steve Frost	E,C&I Professional Lead	
Record Reference:	CM9 Folder 1.1.3.978. (2020/261066)		
Revision commentary:	Rev 4: Routine update Rev 5: Updated Review Period		

TABLE OF CONTENTS

Published 07/19

1. INTRODUCTION AND BACKGROUND

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

2. PURPOSE AND SCOPE

2.1 The purpose of this TAG is to provide guidance to ONR assessors on the interpretation and application of the relevant SAPs when judging the adequacy of the essential services in a nuclear installation.

2.2 The SAPs describe essential services as 'those resources necessary to maintain the safety systems in an operational state at all times, and they may also provide supplies to safety-related systems.' (SAPs paragraph 436).

2.3 Within this TAG the relevant safety systems and safety-related systems which rely on one or more essential services are referred to as structures, systems or components (SSCs). This is illustrated in Figure 1, which highlights a need to first clearly define the safety function to be delivered before defining the safety role for the SSCs, including the attributes of the essential services for those SSCs.

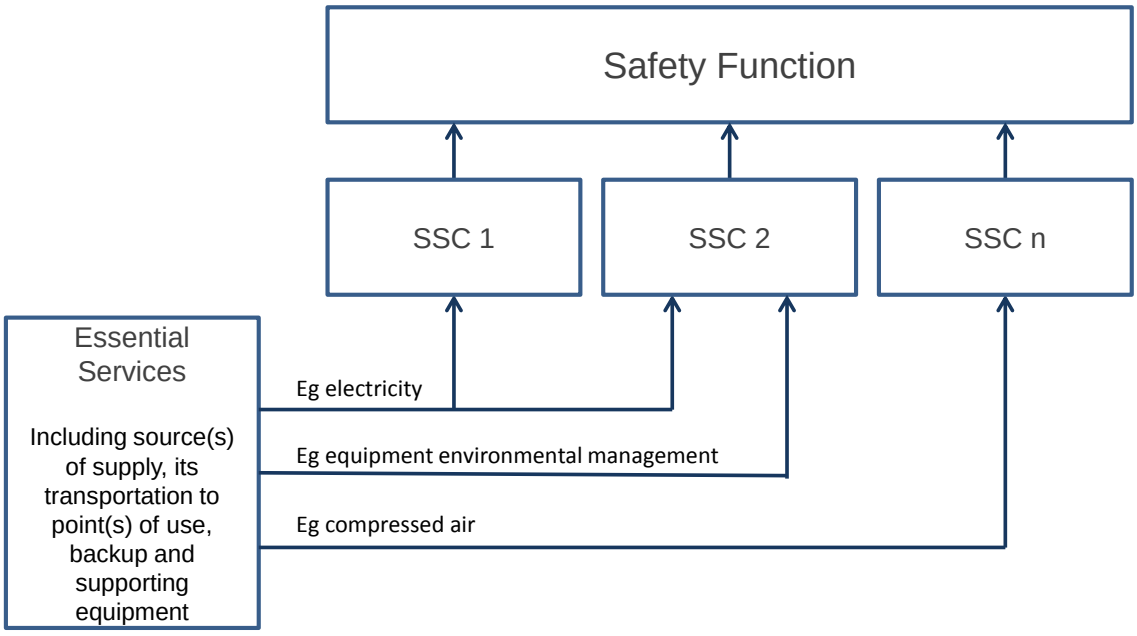

Figure 1 – Essential services role in supporting a safety function

2.4 The term essential services includes the collection of equipment that provides the SSCs with the services they require to perform their safety functions.

2.5 This assessment guide primarily addresses the SAPs Engineering Principles (EES.1 to EES.9) which outline the safety principles to be considered by the assessor when judging the adequacy of the essential services in a nuclear installation. The guide identifies and draws on other relevant key and general SAPs [Ref. 1] which are applicable to the assessment of essential services.

2.6 Other assessment guidance is also available from the IAEA [Refs. 2, 3, 4, 5], which should be appropriately taken into account in conjunction with the application of this guide.

2.7 This TAG is divided into two main sections. The main body contains expectations common to all essential services, while Appendix A lists a non-exhaustive range of typical essential services and sets out expectations specific to each of these.

2.8 This TAG contains guidance primarily to advise and inform ONR staff in the exercise of their professional regulatory judgment. It should be noted that many of these general good practice principles are written in broad terms to cover a range of engineering applications; they are not prescriptive and a fit-for-purpose interpretation may therefore be necessary when applying them to an individual application.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 This section identifies the relationship of essential services to the site licence conditions (LC) [Ref 9]. Under the Nuclear Installations Act 1965, a set of 36 standard licence conditions are attached to each nuclear site licence. These conditions cover the facility lifecycle from design, construction, and operation through to decommissioning and include management oversight and reviews. They require licensees or duty-holders to implement arrangements to ensure compliance. The LCs considered applicable to this TAG are presented below.

- LC 14 (Safety documentation),
- LC 23 (Operating Rules),
- LC 24 (Operating instructions),
- LC 27 (Safety mechanisms, devices and circuits),
- LC 28 (Examination, inspection, maintenance and testing).

3.2 Other potentially relevant licence conditions are:

- LC 10 (Training),
- LC 11 (Emergency arrangements),
- LC 12 (Duly authorised and other suitably qualified and experienced persons),
- LC 15 (Periodic review),
- LC 19 (Construction or installation of new plant),
- LC20 (Modification to design of plant under construction),
- LC 21 (Commissioning),
- LC 22 (Modification or experiment on existing plant).

3.3 It should be noted that essential services may also be subject to regulation by other regulatory bodies. Appendix 1 includes examples of essential services which are also likely to be subject to legislation enforced by another regulatory body, for example EA, SEPA or NRW. Therefore, ONR inspectors should engage with the relevant regulator as necessary.

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

4.1 Engineering principles comprise the major part of the SAPs [Ref 1]. Engineering standards need to be high to achieve the necessary high levels expected for nuclear safety, including under fault conditions. As such, these principles need to be used in combination with the Fault Analysis SAPs. Collectively, the engineering principles should be considered when assessing the safety case for an essential service.

4.2 The following SAPs make explicit reference to the need to consider essential services, including power supplies:

- ECS.2 - Engineering principles: safety classification and standards. Safety classification of structures, systems and components.
- ELO.4 - Engineering principles: layout. Minimisation of the effects of incidents.
- EHA.14 - Engineering principles: external and internal hazards. Fire, explosion, missiles, toxic gases, etc. - sources of harm.
- ESR.6 - Engineering principles: control and instrumentation of safety-related systems. Power supplies.
- ESS.12 - Engineering principles: safety systems. Prevention of service infringement.
- ESR.10 - Engineering principles: control and instrumentation of safety-related systems. Demands on safety systems in the event of control system faults.
- ECH.4 - Engineering principles: chemistry. Monitoring, sampling and analysis.
- FA.14 - Fault analysis: PSA. Use of PSA.
- AM.1 - Accident management and emergency preparedness. Planning and preparedness.

4.3 Several other SAPs are of particular relevance to the assessment of the adequacy of the essential service provisions. The Engineering Principles: essential services (EES.1 – EES.9) are the SAPs which must be considered fundamental to this guide. Since the essential services role is to support SSCs, a number of the SAPs covering Engineering Principles: safety systems (ESS.1- ESS.12) also apply. These SAPs are referred to within relevant clauses of Section 5.

4.4 The following ONR TAGs also provide relevant guidance on aspects such as the role of essential services within an overall defence-in-depth framework, the performance and integrity expectations to support the safety function, design considerations and examination, maintenance, inspection and testing (EIMT) arrangements to ensure equipment continually achieves the expected performance:.

- Safety Systems, NS-TAST-GD-003.
- Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094.
- LC28 Examination, Inspection, Maintenance and Testing (EIMT), NS-TAST-GD-009.
- Probabilistic Safety Analysis, NS-TAST-GD-030.
- Limits and Conditions for Nuclear Safety (Operating Rules), NS-TAST-GD-035.
- Diversity, Redundancy, Segregation and Layout of Mechanical Plant, NS-TAST-GD-036.
- Design Safety Assurance, NS-TAST-GD-057.
- Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), NS-TAST-GD-005.
- Internal Hazards, NS-TAST-GD-014.
- Pressure Systems Safety, NS-TAST-GD-067.
- Emergency Power Generation, NS-TAST-GD-103

WENRA Safety Reference Levels

4.5 WENRA Reactor Safety Reference Levels [Ref. 8] consider the safety requirements for existing reactors. The following areas are relevant to Essential Services:

- Issue E: Design Basis Envelope for Existing Reactors
- Issue F: Design Extension of Existing Reactors
- Issue G: Safety Classification of Structures, Systems and Components
- Issue H: Operational Limits and Conditions
- Issue I: Ageing Management
- Issue K: Maintenance, In-Service Inspection and Functional Testing
- Issue LM: Emergency Operating Procedures and Severe Accident Management
- Issue O: Probabilistic Safety Analysis
- Issue P: Periodic safety Review (PSR)

- Issue Q: Plant Modification
- Issue R: On Site Emergency Preparedness
- Issue T: Natural Hazards

4.6 In considering the design of new Nuclear Power Plants (NPP), the WENRA Reactor Harmonisation Working Group (RHWG) Report, Safety of new NPP designs, March 2013, makes reference to essential services in that their design:

- Should not unduly compromise the independence of the SSC they actuate, support or interact with.
- Should consider multiple common cause failure events or inefficiencies of an essential service to fulfill a required safety function necessary to cope with normal operations, anticipated occurrences and faults

IAEA Safety Standards

4.7 IAEA Specific Safety Requirement No. SSR 2/1 (Rev 1.) [Ref. 3] Requirement 27 makes reference to essential services in that:

- They shall be classified accordingly.
- Their reliability, redundancy, diversity and independence and the provision of features for their isolation and for testing their functional capability shall be commensurate with the significance to safety of the system being supported.
- Their failure should not be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions and compromising the capability of these systems to fulfil their safety functions.

4.8 The IAEA Safety Guide No SSG-34 Design of Electrical Power systems for Nuclear Power Plants [Ref. 10], makes reference to the necessary characteristics of electrical power systems for nuclear power plants and of the processes for developing these systems, in order to meet the safety requirements of SSR-2/1 [Ref. 3]

4.9 IAEA TECDOC No. 1770 Design Provisions for Withstanding Station Blackout at Nuclear Power Plants [Ref. 4], makes reference to electrical power systems and the defence in depth concepts to be applied.

4.10 IAEA Safety Guide No. NS-G-1.7. Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants (2004) [Ref. 5], makes reference to structures, systems and components important to safety and their requirement to be designed and located to minimise the likelihood and effects of internal fires and explosions caused by external or internal events.

4.11 The IAEA guide for Instrumentation and Control (I&C) Systems Important to Safety in Nuclear Power Plants [Ref. 6] is also relevant. This is not only because it highlights the importance of considering the role of essential services in supporting front line I&C systems, but also because it sets out a good practice approach consistent with NS-TAST-GD-094 in defining and substantiating the safety functional requirements of a system. Similar principles can be applied to essential services.

5. ADVICE TO INSPECTORS

General

5.1 Within this TAG the relevant safety systems and safety-related systems which rely on one or more essential services are referred to as SSCs. This is illustrated in Figure 1, which highlights a need to first clearly define the safety function to be delivered before defining the safety role for the SSCs, including the attributes of the essential services for those SSCs.

5.2 The fundamental purpose of essential services is the provision of those services necessary to support safety functions which may be called on to ensure safety on the nuclear installation throughout its lifecycle. The purpose of the assessment is to confirm, with regard to essential services, that the licensee can demonstrate that:

- they are correctly functionally categorised and safety classified according to their safety significance,
- they possess the relevant attributes commensurate with the safety significance including capacity, duration, availability, resilience and reliability,
- the relevant essential service attributes have been identified for all stages of a plant's lifecycle, including decommissioning.
- a relevant analysis has considered all ancillary equipment needed to ensure the essential service can be delivered (e.g. pumps, valves, cooling water), and,
- they are able to perform their function in any environment they may be exposed to in either normal or identified accident conditions for a specified time. This should include the effects of failure of surrounding equipment such as civil structures (e.g. walls, pipe bridges) and non-essential pipelines.

5.3 The assessment process consists of a comparison of the duty-holder's arrangements against relevant good practice. ONR considers relevant good practice (RGP) to be taken from national and international guidance on essential services and includes this TAG. From this a judgement can be made regarding the regulatory confidence in the demonstration of safety via a suitably derived set of clear and coherent safety claims supported by cogent arguments which can be adequately evidenced. This TAG highlights the main considerations for an essential services assessment. Owing to the breath of the topic, inspectors leading assessment activities should consider the need to engage and obtain advice from other appropriate specialists.

5.4 There is an expectation that the duty-holder will explicitly highlight non-conformance with relevant good practice and provide justification within the safety case for how it has reduced relevant risks so far as is reasonably practicable. For example, where older facilities may have been designed and constructed to engineering standards which have been superseded, this may alter the options available when considering the reasonably practicable measures. See also NS-TAST-GD-005 for guidance on the Demonstration of ALARP.

Functional Safety Definition

5.5 The safety submission from the licensee should clearly identify and define essential services that are necessary to ensure safety. The safety submission should also define the required performance of each essential service as well as demonstrating the adequacy of its capacity, duration, availability, resilience and reliability to meet the maximum demands of its dependent systems (EES.3), as is necessary to ensure the maintenance of a safe plant state in normal operation and in fault and accident conditions (EES.1). For each SSC, it should also define those essential services which are required and identify the source. It should be noted that duty-holders use various terms for essential services (e.g. duty, normal, preferred, backup, alternative, emergency). The following SAPs are relevant when considering the adequacy of the functional safety definition:

- FA.2 - Identification of initiating faults,
- FA.6 - Fault sequences,
- FA.8 – Linking of initiating faults, fault sequences and safety measures,
- ECS.1 - Safety categorisation,
- EHA.1 – Identification and characterisation,
- FA.9 – Further use of DBA,
- ESS.11 – Demonstration of adequacy.

Demonstration of Claims

5.6 It should be confirmed that the essential service will be maintained for a sufficient period to bring the plant to a safe state and maintain it in this condition:

- EES.3 describes the relevant attributes of the essential service to include its capacity, duration, availability, resilience and reliability to meet the maximum demands of its dependent systems.
- FA.8 describes the relevant attributes of the essential service to be capable of bringing the facility to stable, safe state following any design basis fault, inclusive of mission times for SSCs or time taken to introduce alternative equipment for longer term safety function provision.

5.7 SAP ECS.2 expects essential services that support components of a safety or safety-related system to be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of its safety functions.

5.8 It is helpful to refer to Figure 1 to illustrate this point. Failure of one essential service (e.g. compressed air) may be an initiating event that does not prejudice successful delivery of another essential service or the relevant SSC (e.g. SSC n), in which case this essential service could attract a lower classification than the SSC it supports. In contrast, the success of SSC 2 might be largely dependent on the water essential service, in which case this essential service would be expected to be classified identically to SSC 2. The resulting safety classification should be supported by a robust demonstration that SAP ECS.2 expectations have been met.

5.9 The potential for over-classification of essential services can be avoided by providing greater clarity regarding the specific safety functions attributable to the engineered system that will be subject to classification See also the guidance provided in NS-TAST-GD-094 on Categorisation of Safety Functions and Classification of Structures, Systems and Components.

5.10 Duty-holders should demonstrate that they have given particular attention to the potential for essential services to undermine the independence of SSCs. This includes reasonably foreseeable multiple or dependent faults, such as the loss or degradation of one essential service interrupting another essential service. The failure mode of the SSC on loss of each essential service (which may potentially be a source of common cause failure) should also be assessed by the licensee (EDR.1).

5.11 It is important for the essential service supply equipment to feature appropriate levels of redundancy, diversity and segregation (EDR.2, ESS.18, ELO.1) commensurate with the safety classification (ECS.2) and reliability claims made on it (ERL.1-ERL.4). Common cause failure is expected to limit the reliability claims on even simple SSCs with built in redundancy to $1x10^{-5}$ (see EDR.3). In practice, more modest claims on reliability may be appropriate, particularly where control systems are required to achieve correct operation of the essential service, even if the SSC in question carries a high safety classification See also the guidance provided in NS-TAST-GD-046 on Computer Based Safety Systems.

5.12 It is expected that the consideration of the effects of adverse conditions and faults in the essential service (e.g. the normal supply, the back-up supply, the distribution of the service) should be analysed and the design shown to have incorporated adequate provision to ensure that the reliability of the essential service is not compromised (EES.6, ESS.18). This should include the impact of internal hazards such as vehicle impact and external hazards such as lightning (EHA.1). This should also include appropriate on-line or off-line sampling arrangements to provide confidence that the quality of the essential service meets the specification (e.g. purity, concentration (ECH.4) See also the guidance provided in NS-TAST-GD-088 on Chemistry of Operating Reactors and NS-TAST-GD-089 on Chemistry Assessment.

5.13 The minimum permitted configurations of essential supplies systems should be stated and the adequacy of that state justified. For the permitted minimum configurations, it should be confirmed that the expectations of the single failure criterion (EDR.4) are met where the essential supplies support the principal means of fulfilling a Category A safety function.

5.14 The remainder of this section provides further guidance regarding ONR's expectations for demonstration of adequate essential services.

Sources of Supply

5.15 Where any essential service supply is derived from a source external to the nuclear site, that supply should also be obtainable from a suitably independent and diverse back-up source on the site (EES.2). An important consideration here is the extent to which the source is under the direct control of the licensee. For example, an extended regional loss of grid may not only impact on the electricity supply to the site but may also interrupt tanker deliveries of diesel fuel supplies needed to power on-site back-up generators.

5.16 Each back-up or alternative source of an essential service should be considered to confirm that it has the necessary capacity, availability and reliability to meet the maximum demands on it, and can provide that service for the necessary time (EES.3). SAP EES.9 includes an expectation for the duty-holder to demonstrate, with reference to the likelihood and consequences of simultaneous loss of normal and back-up

sources, that it is not reasonably practicable to add further back-up provisions to the design.

5.17 The adequacy of the means used to deliver the service from source to destination (eg pipes/cables) will also need to be assessed using similar principles.

Shared Essential Services

5.18 Where multiple facilities make use of any essential service, the means by which the essential service provision is prioritised when a fault or excess demand occurs in the other facilities should be defined and assessed to confirm its effectiveness and reliability. In the particular case of several plants sharing a common service, the effect of that sharing should be incorporated into the definition of capacity etc. and considered when assessing the adequacy of the service (EES.4, EES.5). The classification of the shared essential service should be determined by considering the system with the highest safety classification required (e.g. Class 2 would be expected if one plant required Class 2 even if all the other plants required Class 3). The protection system associated with the sharing should be assessed to confirm its effectiveness and integrity. In those cases where there is a site-wide essential service, a safety case should be provided to justify the adequacy of the central essential services, and this safety case should identify and tabulate the totality of the site essential service requirements and demonstrate that these can be provided.

5.19 Some shared services, such as site utilities, may potentially perform a dual role whereby their provision is necessary for operational production purposes and also for preventing a demand being placed on safety measures needed for the continuation of the safety function. It is therefore important that a clear definition of the boundaries of each essential service and its source(s) should be established for analysis. Each service should be subject to analysis to confirm that it will be protected from faults that occur within itself or in an SSC that it supports, such that its availability to support safety functions is assured so far as is reasonably practicable. EES.7 is directed particularly at this requirement to minimise the probability of the essential service being lost, which is consistent with the expectations of SAPs EKP.2, ELO.1 and ELO.2.

Defence in Depth Principle

5.20 In accordance with the defence in depth principle covered by EKP.3, the expectation is for the provision of multiple independent barriers to fault progression. A clear distinction therefore has to be maintained in the safety case between the role of essential services equipment that support SSCs at each of the defence in depth levels. The key essential services SAPs include SAPs EES.1 and EES.12. Guidance on prevention versus protection is provided in section 5.6.4 of NS-TAST-GD-094 (ONR TAG - Categorisation of Safety Functions and Classification of Structures, Systems and Components).

5.21 The focus should be on preventing a fault occurring (defence in depth Levels 1 and 2) and thereby limiting the demand on protection measures. The integrity of the essential services equipment supporting a preventative SSC should not be lowered simply because protective measures exist. Similarly, the integrity of the essential services equipment supporting an SSC providing protection within the design basis against escalation to an accident (defence in depth Level 3) should not be lowered because beyond design basis accident management and emergency preparedness measures exist (defence in depth Levels 4 and 5). The defence in depth principle requires design to incorporate sufficient diversity and segregation to avoid the effects of common cause failure (EDR.3, EQU.1 and EES.6).

Human Factors and Operating Instructions

5.22 The adequacy of the administrative, human and organisational factors aspects of the overall essential services systems should be considered (EHF.1 – EHF.12, ESS.8 and ESS.9). This includes aspects of the allocation of safety actions between humans and engineered systems, including the requirement for automatic or manual initiation of back-up service provision.

5.23 The requirements for the availability of essential services should be specified in the plant operating rules, identified operating instructions, and plant operating and maintenance instructions as appropriate. Adequate training and exercises should be in place to ensure that operators have sufficient information available to them to take appropriate actions under all postulated conditions. The need for the clear identification of equipment, devices or systems, and the security arrangements (e.g. lockable cabinets, valves) for the essential services should be considered.

Equipment Qualifications and System Validation

5.24 Where an essential service and hence its supply and distribution equipment is important to safety, the licensee should qualify it (EQU.1) for the range of normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lifetime.

5.25 The qualification basis of the essential services should be stated, and it should be demonstrated that they meet relevant standards and are adequate for all anticipated fault and environmental conditions (EHA.1, ECS.2, ECS.3 and ECS.4). In particular, the basis of seismic qualification should either be stated in the safety case, or any absence of such qualification noted and justified.

5.26 Confirmation of the availability of essential services should be validated through the use of objective evidence (e.g. analysis, end-to-end testing, inspection, exercises, events) that will meet the objectives and requirements claimed (ESS.11). This should include all claims made on administrative arrangements to maintain services or restore lost services in accordance with written instructions.

5.27 Equipment qualification and system validation claims for essential services, their supply and their distribution equipment important to safety during severe accident scenarios shall only be made if those essential services, their supply and their distribution equipment important to safety are available during those scenarios.

5.28 The licensee's arrangements should support the opportunities to confirm the engineering and administrative arrangement for essential services meets their safety performance requirements. This may include gaining confirmation that the loss of the particular service provision does not have safety significance.

Environmental Management

5.29 Essential service systems and equipment includes that which manages, controls or monitors the environmental conditions required for the successful operation of components of a safety or safety-related system (including environmental conditions to allow claimed human actions to be carried-out). Such systems and equipment should therefore be classified accordingly unless their failure does not prejudice successful delivery of the associated safety function (ECS.2).

5.30 A number of SAPs refer to the expectation that the anticipated range of environmental conditions that SSCs will be subjected to over the lifetime of the plant, including different operational, fault and accident conditions, should be analysed, defined, and substantiated. Specific expectations include:

- The SSC capability should exceed that necessary for the effective delivery of the safety functions in the prevailing operating environment by a clear margin (ESS.10).

- Qualification procedures applied to structures, systems and components should address all relevant operational, environmental, fault and accident conditions (EQU.1).

- The reliability claimed for any structure, system or component should take into account its novelty, experience relevant to its proposed environment, and uncertainties in operating and fault conditions, physical data and design methods (ERL.1). Any reliability claims made against an SSC should be demonstrated by suitable analysis of both random and systematic failures (ERL.2).

- Where appropriate, the heating, ventilation and air conditioning (HVAC) design and the associated safety justification should include the provision of a suitable working environment for personnel and structures, systems and components, particularly in the control rooms (ECV.10).

- Where prevention, or an acceptably low likelihood of infringement of a service, cannot be demonstrated (e.g. environmental conditions within acceptable limits), features should be incorporated to ensure a failsafe outcome (ESS.12).

Maintenance, In-Service Inspection and Functional Testing

5.31 The design of essential services should demonstrably allow for routine maintenance, testing and monitoring throughout the lifetime of the station/plant and meet any probabilistic risk analysis requirements. The maintenance, testing and monitoring requirements should be specified in the maintenance schedule and detailed in the associated maintenance instructions. Essential services might be taken out of service for maintenance, testing and monitoring requirements during normal plant operations. In this case, operating rules (LC23) should state the minimum requirements for safe operation.

5.32 The main points to be considered in respect of the essential services relate to commissioning, maintenance, inspection, testing, sampling and monitoring and plant operation (EMT.3, EMT.5, EMT.6, EMT.7, ELO.1, ECH.4 and EAD.4).

Management of Plant Ageing

5.33 The SAPs include a section, namely EAD.1- EAD.5 on ageing and degradation, which addresses the need to identify the actions necessary to ensure that an adequate standard of safety will be maintained over the lifetime of the plant.

5.34 It should also be noted that numerous discipline-specific standards and sources of relevant good practice exist to define the processes that should be adopted throughout the lifecycle of a facility. In addition, WENRA reference levels [Ref. 8] state that the design shall take into account the effects of operational conditions over the lifetime of the plant and, when required, the effects of accident conditions on their characteristics and performance.

Impacts from Internal Hazards

5.35 The SAPs include a section (EHA.1 – EHA.19) which addresses the need to identify and minimise the effects of internal hazards (e.g. fire, internal flooding, missiles and dropped loads). This is to ensure internal hazards do not adversely affect the reliability of safety systems to perform essential safety functions. Items important to safety (i.e. essential services) should be either protected against the hazard by appropriate use of segregation, redundancy, diversity and separation, or qualified to withstand the effects of the hazards.

Effect of Plant Modifications

5.36 As the plant is operated and modified, changes will be made which will affect the need for and provision of essential services. As such changes may have been considered in isolation, the duty-holder should have arrangements for the regular comprehensive review of the effects of modifications on the essential services and the demands placed on those services. The objective of this is to confirm the continued ability of the essential services to adequately support the relevant SSCs.

Non-Nuclear Safety

5.37 Essential services and associated equipment may give rise to a range of conventional safety hazards (e.g. asbestos, chemicals, confined spaces, construction, electrical, fire and explosion, flammable liquids and gases, legionella, lifting equipment, machinery, noise, pressure systems, sewage, transport). ONR inspectors leading assessment activities should consider the need to engage and obtain advice from appropriate non-nuclear specialists, see also NS-INSP-GD-051 for guidance on the Regulation of Conventional Health and Safety on GB Nuclear Sites.

6. REFERENCES

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

2 WENRA Reactor Harmonisation Working Group (RHWG) Report, Safety of new NPP designs, March 2013. http://www.wenra.org/publications/

3 IAEA Specific Safety Requirement 2/1 Safety of Nuclear Power Plants Design (Rev 1), 2016. https://www.iaea.org/publications/10885/safety-of-nuclear-power-plants-design

4 IAEA TECDOC No. 1770 Design Provisions for Withstanding Station Blackout at Nuclear Power Plants http://www-pub.iaea.org/MTCD/Publications/PDF/TE-1770_web.pdf

5 IAEA Safety Guide No. NS-G-1.7. Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants (2004). http://www-pub.iaea.org/MTCD/publications/PDF/Pub1186_web.pdf

6 IAEA Specific Safety Guide No. SSG-39. Design of Instrumentation and Control Systems for Nuclear Power Plants (2016). http://www-pub.iaea.org/MTCD/publications/PDF/Pub1694_web.pdf

7 IAEA-TECHDOC-1787. Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants (2016). http://www-pub.iaea.org/MTCD/publications/PDF/TE-1787_Web.pdf

8 Western European Nuclear Regulators' Association WENRA. Reactor Harmonization Group. Safety Reference Levels for Existing Reactors – 24 September 2014. http://www.wenra.org/publications/

9 Licence condition handbook. Office for Nuclear Regulation. February 2017. http://www.onr.org.uk/documents/licence-condition-handbook.pdf

10 The IAEA Safety Guide No SSG-34 Design of Electrical Power systems for Nuclear Power Plants https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1673web-53477409.pdf

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

7. GLOSSARY AND ABBREVIATIONS

AC	Alternating current
DC	Direct current
EIMT	Examination, inspection, maintenance and testing
HVAC	Heating, ventilation and air conditioning
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
LC	Licence condition
ONR	Office for Nuclear Regulation
PSA	Probabilistic safety analysis
SAP	Safety assessment principle(s)
SSC	Structures, systems and component
TAG	Technical assessment guide(s)
WENRA	Western European Nuclear Regulators' Association

8. APPENDICES

8.1 APPENDIX A –ESSENTIAL SERVICES EXAMPLES

8.1.1 For each essential service, the design and attributes of the facilities for its supply, storage and distribution should be assessed against the expectations in the main body of this TAG. This appendix contains a number of considerations specific to particular essential services. These are not exhaustive and it is recommended that further advice is sought from relevant specialists.

8.1.2 Essential systems containing a fluid under pressure must comply with the Pressure Safety System Regulations (PSSR). Guidance is provided in NS-TAST-GD-067 – Pressure Systems Safety. Failure of pressurised parts results in a release of stored energy that can cause widespread effects on site due to the generation of missiles.

Water Supplies

8.1.3 Water can be supplied to the site from a number of sources; for example, town's water, local reservoirs/lakes and the sea. An analysis of the requirements for water supplies, both in terms of quantity and quality, should be made in the safety case. Where the supply is required for an essential service (e.g. emergency boiler feed systems) the on-site alternative supply should be provided from a dedicated facility (e.g. reservoir, storage tanks) and minimum supply holdings justified and demonstrated.

8.1.4 Consider an example where the loss of the site water supply for a defined period may be acceptable if a back-up local water storage tank is able to passively provide the essential water service during the duty system outage period. If the local storage tank can provide all of the attributes for the essential service (ie capacity, duration, availability, resilience and reliability) this may allow the site water supply to be considered as a safety-related system rather than part of the safety system and may therefore justify a lower classification than the local storage tank system. In this case the classification of the site water supply is determined by the fact that its failure could threaten safety by placing a demand on a safety system (ie provided by the attributes of the back-up water tank system). Alternatively, restoration of the site water supply may be needed to bring the plant to a safe state and maintain it there. This would lead to a need for higher integrity in the engineering and administrative arrangements for the restoration of the site water supply; these arrangements would therefore need to be considered part of the same essential service delivery system as the local storage tank and all parts of this system would attract a higher classification.

8.1.5 If the storage or distribution facility is in any way shared, the supply to any non-essential service should be designed such that it does not affect the minimum storage requirements assumed in the safety case.

8.1.6 The provision of all water supplies defined as relevant to nuclear safety should be shown to be independent of any supplies required for non-nuclear safety related firefighting purposes.

8.1.7 Essential cooling water supplies should be defined in the safety submission, and particular care should be taken to confirm that any essential service attributes of any auxiliary cooling water systems are defined and demonstrated.

8.1.8 Where essential cooling is provided by cooling towers or other air heat exchangers, the safety case should justify any dependencies on any other essential supplies such as electrical systems.

Drainage Systems

8.1.9 These systems are designed to collect, transport, store, treat and discharge waste water and surface water to ensure the continued safety and operability of the site. These systems are designed to collect, transport, store, treat and discharge waste water and surface water to ensure the continued safety and operability of the site. The duty-holder should demonstrate that in accordance with SAP ECS.2 it has used appropriate processes to determine the classification of the SSCs that comprise the drainage system. Drainage systems that deliver safety functions should be considered as Essential Services unless otherwise justified by the duty-holder.

8.1.10 The duty-holder should demonstrate that surface water drainage systems meets SAP EHA.15 expectation that the design and maintenance of the facility should prevent water from adversely affecting structures, systems and components important to safety (See ONR TAG regarding Internal Hazards, TAG NS-TAST-GD-014). The duty-holder should consider potential surface water flooding initiating events and demonstrate that the drainage systems are adequate to limit the extent and frequency of surface water flooding.

8.1.11 The duty-holder must take reasonable measure to prevent waste water entering the surface water drainage system. For example, to mitigate against spread of activity, some surface water drains discharge to sumps where the collected water must be sampled and tested for activity prior to pumped discharge into the gravity feed surface water drainage system.

8.1.12 The duty-holder should demonstrate that the waste water drainage system meets SAP ECV.1 expectations that the design and maintenance of the drainage network should ensure that radioactive material is contained and generation of radioactive waste through the spread of contamination by leakage is prevented.

8.1.13 Note the relevant environmental regulator will provide enforcement in relation to the discharge of radioactive waste from nuclear sites.

Compressed Air Supplies

8.1.14 These will normally be provided via a compressor, storage vessel and distribution pipework. In some cases the essential supply may be claimed as, or supported by, a central or distributed system of transportable pressure receptacles containing compressed air (air cylinders), or by cross-connection to lower quality air systems, for example factory or general purpose air.

8.1.15 The integrity of the compressed air supply should not be undermined by making cross-connections (EES.5). Consideration should be given to the:

- Segregation and independence of the normal and essential air systems to ensure that the effects of internal hazards and system failures are adequately addressed.

- Segregation and independence from other systems important to safety to ensure that pressure hazards and random failures (eg leaks) do not degrade the system.

8.1.16 It should be ascertained that the capacity of the storage vessels is adequate to supply the SSCs (typically instrumentation) for the required period, and that the quality of the air supply will not degrade the performance of the equipment. In particular, it should be noted that an unsuitable air composition (eg moisture and/or oil content) may have latent and/or long lasting detrimental effects on the reliability of system and the SSC it operates.

8.1.17 When assessing compressed air supplies, attention should be given to the requirements for electrical supplies, cooling water supplies and any other essential services necessary to support the compressors.

Steam Supplies

8.1.18 Where there is an identified requirement for an essential steam-raising supply (e.g. to vaporise carbon dioxide) the arrangements for the boiler fuel supplies (for starting and running), boiler ignition, feed water supplies and any auxiliary steam supplies should each conform to the essential services principles stated variously above. In particular, an assessment should be made of the boiler's capability to supply its demanded capacity in the event of a loss of site electrics.

8.1.19 As with other pressurised systems, consideration should be given to failure resulting in a release of stored energy. Other local effects can be scalding of personnel and serious damage to plant caused by high temperatures or ingress of steam (eg ventilation systems might be rendered inoperable if their filters are wet).

Gas Supplies

8.1.20 Gas required for safety systems, such as carbon dioxide and nitrogen, is normally delivered to site by road tankers or in transportable pressure receptacles (gas cylinders) depending on the nature and volume of the gas.

8.1.21 To provide an alternative supply on the site, it is necessary to ensure that the storage facilities are adequately sized in order that the fault study assumptions are still met in the event of an interruption of the routine deliveries. Therefore, it is necessary to have established the minimum on-site holdings of gas supplies for continued safe operation.

8.1.22 When assessing such essential gas supplies, attention should be given to any supply requirements for steam or electrical heating that vaporises or conditions the gas before distribution. The likelihood and consequences of extreme temperature being experienced by the distribution system should also be considered. The condition of vacuum insulated vessels and associated equipment for maintaining the vacuum should also be examined. Spillages of very cold liquids can cause embrittlement and subsequent failure of certain materials, e.g. carbon steel.

Lubricants

8.1.23 Adequate lubrication of moving/rotating safety-related plant and equipment should be considered by the inspector both from the design and maintenance viewpoints. For example, when evaluating safety significant cooling circulating pumps that are lubricated by a circulating oil system, diversity of electrical supply to the pump motors should be considered. In practical terms, minimum stocks of lubricants are unlikely to be a problem, but if the system inventory is small, licensees would be expected to have a minimum stock policy. Suitable arrangements should be in place to ensure a single contamination episode of any stored lubricant cannot lead to multiple equipment failure. Regular monitoring of lubricant properties should take place to ensure that they have not degraded or have become contaminated.

Fuel

8.1.24 In this context, fuel is typically required for the essential electrical generators, usually diesels or gas turbines, and for steam-raising for vaporisation of carbon dioxide or in some cases reactor start-up (to warm up pressure vessels). See ONR TAG regarding Emergency Power Generation Systems NS-TAST-GD-103.Special attention should be paid to the fuel pipe and valve supply arrangements and to the storage tank segregation to ensure that a common mode fuel supply fault to the prime movers cannot occur.

8.1.25 The duty-holder should have suitable arrangements in place to ensure that the appropriate quality of fuel is delivered and maintained whilst in the storage tanks, including avoidance of degradation due to fuel ageing. The aim is to ensure that no single fault (eg contaminated or wrongly specified fuel) will cause a multiple failure of the prime movers. This is typically achieved by phased delivery of fuel into segregated storage tanks and avoiding fuel transfers between these storage tanks.

8.1.26 Additionally, adequate risk assessments are required in areas where there are dangerous and explosive substances present, under the requirements of the Dangerous Substances and Explosive Atmosphere (2002), (DSEAR) Regulations and other relevant regulations.

Electrical Supplies

8.1.27 The IAEA provide relevant guidance on the design of power systems for nuclear power plants [Ref. 4] which supports the essential services expectations contained in SAPs EES.1 to EES.9. The foreword of this document highlights that it is not only relevant to nuclear power plants but also other types of nuclear facilities. This IAEA guide includes the following expectations:

- The electrical essential service is normally derived externally (e.g. from the National Grid) with the on-site electrical power distribution network providing the normal means of delivering power from the off-site power source to support the requirement of the SSC (Note that non-safety loads would also be supplied from the same power distribution network).

- In the case of loss of off-site power, an onsite standby AC power source is used (e.g. diesel or gas turbine driven generators). Non-safety loads are generally disconnected when the preferred power supply is not available in order to avoid overloading the on-site power sources and to prevent faults in the non-safety systems from degrading the on-site power sources. Assessors should confirm that adequate provision is made for the starting of these generators, the disconnection of non-safety loads, the connection of essential loads and any necessary alterations to electrical distribution networks.

- A loss of all AC power (a Station Black Out or Site Black Out for non-power reactor sites) needs to be accommodated. The loss of all AC power would result from the loss of off-site power and loss of standby AC power sources. An independent alternate AC power source is expected to re-supply the SSCs within the time needed to maintain plant safety and to be maintained or be resilient for the duration of the loss of AC power. In this situation the expectation is for relevant storage (e.g. battery) systems to be designed to supply vital control and instrumentation systems with power until the independent alternate AC power source can be restored.

- An adequately equipped emergency control centre with its own autonomous power system, emergency plans and emergency procedures for onsite and offsite emergency response.

8.1.28 Whist the IAEA guide [Ref. 4] provides relevant electrical engineering expectations, assessment should primarily be against ONR SAPs and TAGs. For example, informed by the frequency or consequences, the reasonably practicable approach (in accordance with SAP EES.9) may be to adopt more or less redundancy or diversity in the electrical essential service provision or to provide other SSCs that support the relevant safety function(s).

8.1.29 It should be noted that the IAEA has provided worked example guidance [Ref. 7] on the classification of structures, systems and/or components and this includes those in relation to loss of off-site power for civil nuclear reactors.

8.1.30 It should also be noted that WENRA Reference Levels for existing civil nuclear reactors [Ref. 8] gives specific expectations for emergency power supplies during various operational and accident states.

8.1.31 Some loads may be tolerant to a short supply interruption and can therefore be connected to an interruptible AC supply. This is typically required for a restricted range of major motive power applications such as emergency boiler feed pumps, low speed gas circulator drives, larger essential ventilation systems and essential cooling water supplies. However, some loads cannot tolerate interruption and therefore require AC or DC uninterruptable supplies, as is the case for:

- lighting and communications systems,
- motors driving critical cooling pumps and critical ventilation systems,
- monitoring instrumentation such as criticality detectors, reactor instrumentation, radiation detection and plant and power reactor shutdown and control systems,
- valve actuators required to isolate damaged sections of the plant and activate alternative cooling circuits,
- heating, cooling and ventilation systems needed to maintain the quality of air in equipment rooms, control rooms and to remove contaminated air to suitable filter systems, and
- electrical relays used to trip and initiate electrical switchgear, and those handling the unloading of normal supplies from the system to allow the essential electrical supplies to be brought into operation.

8.1.32 Each electrical supply source should have the capacity, duration, availability, resilience and reliability to meet the maximum demands of its dependent systems (EES.3). Electrical analysis should be carried out to ensure that the electrical supply, generators and distribution networks are capable of delivering the maximum electrical loading requirements and to determine system resilience to faults and disturbances. Electrical analysis should include:

- load flow analysis to ensure that the supply can meet the demand under normal operation and during the restoration of drives when the alternative supply has been established,
- electrical fault analysis to determine the expected fault currents under earth fault and short-circuit conditions, including fault protection discrimination studies,
- transient stability studies, and
- Voltage studies to ensure that voltages at all parts of the system are within the tolerance to operate the electrical plant and equipment. This includes

considerations such as the starting of large motors, the effect of long circuits and the potential voltage rise from local generators or capacitors.

8.1.33 The effects of loss of normal (off-site) and on-site AC electrical power should be addressed to ensure that the plant is maintained in a safe state in normal operation and in fault and accident conditions (EES.1). The general expectation is that loss of all off-site electrical supplies up to 24 hours should be treated as a frequent fault (>1 x 10^{-3} /yr) and for losses up to a week as an infrequent fault (>1 x 10^{-5} /yr).

8.2 APPENDIX B – WENRA REFERENCE LEVEL MAPPING

Table 1 shows the most significant mapping of the safety reference levels for operating reactors [Ref. 8] to the relevant sections of this ONR Technical Assessment Guide. All aspects of the mapping is not show since aspects of this TAG relate to multiple reference levels and other ONR guidance can have stronger relevance to the particular reference level

Reference Level		TAG Section	Comment
A	Safety Policy	-	
B	Operating Organisation	-	
C	Management System	-	
D	Training and Authorization of NPP Staff (Jobs with Safety Importance)	-	
E	Design Basis Envelope for Existing Reactors	Section 5	
F	Design Extension of Existing Reactors	Section 5	
G	Safety Classification of Structures, Systems and Components	5.6	
H	Operational Limits and Conditions	5.24	
I	Ageing Management	5.34	
J	System for Investigation of Events and Operational Experience Feedback	-	
K	Maintenance, In-Service Inspection and Functional Testing	5.32	
LM	Emergency Operating Procedures and Severe Accident Management Guidelines	-	
N	Contents and Updating of Safety Analysis Report	-	
O	Probabilistic Safety Analysis	-	
P	Periodic Safety Review	-	
Q	Plant Modifications	5.36	
R	On-site Emergency Preparedness	-	
S	Protection against Internal Fires	-	
T	Natural Hazards	-	

TABLE 1 - CROSS-REFERENCES TO WENRA REFERENCE LEVELS