NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM		
TECHNICAL ASSESSMENT GUIDE **CONTAINMENT: ESSENTIAL SERVICES**		**T/AST/019** ISSUE 001
Approved By: *J Cowley*	J Cowley	Issue Date: 12/11/99
Open Government Status: Fully Open		Review Date: 12/11/02

Contents

1. Purpose and scope

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

1.2 The Essential services are the collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection and safety actuation systems and are thus an integral support to the safety functions in an operational state at all times.

1.3 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 the lifecycle. The purpose of the assessment is to confirm the Licensee has demonstrated that :

1) the need for essential services has been identified for all stages of a plant's lifetime, including decommissioning and correctly categorised according to their safety significance,

2) they will be available when a demand is placed upon them,

3) they have the capacity to supply the service during normal operation and all identified fault conditions,

4) 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 non-essential equipment such as masonry walls, turbines, pumps, etc.

5) the analysis has all ancillary equipment needed to ensure the service can be delivered, i.e. pumps, valves, cooling water etc.

1.4 These requirements must be met for all of the services which are considered to be essential for the safe operation and shut-down of the nuclear facility and may include electricity supplies, water, gases, fuels and lubricants, and any others as may be specified in the safety case.

1.5 This assessment guide addresses the general engineering principles (P214 to P221) 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 **[1]** which are applicable to the assessment of essential services.

1.6 Other assessment guidance is also available from the IAEA Safety Series of publications. The relevant guide in this series **(Ref. 2)** was revised and reissued in 1991, and had a major input from the NII; the assessor should also therefore be satisfied that, as a minimum, the

recommendations of the guide are met.

1.7 This TAG contains *guidance* to advise and inform NSD inspectors in the exercise of their professional regulatory judgement. Comments on this guide, and suggestions for future revisions, should be recorded on the appropriate registry file.

2. SAPs addressed

2.1 The essential services Principles (P214 - P221) are the ones which must be considered fundamental to this guide.

2.2 Three Safety Analysis principles are also of particular relevance as they identify the key information inputs to the assessment of the adequacy of the essential service provisions :-

P16 - Requires an analysis of initiating faults.

P22 - Requires the identification of these faults.

P26 - Requires the establishment of a schedule of safety systems and minimum safety system requirements.

2.3 As a sound provision of Essential Services depends on the application of good engineering principles, many of the other SAPs will be considered during the assessment of the plant or the design. In analysing the essential services provisions, the assessor should also take into account the following key engineering principles:-

P62 - Sensitivity to fault should be minimised.

P65 - Defence in depth.

P68 - Redundancy and diversity are expected.

P69 - Safety Categorisation for systems or components.

P72 - Internal and external hazards which may affect the essential services.

P73 - Availability of safety systems (and by implication any essential services on which they depend) and separation of safety systems from control systems.

P74 - Layout to minimise effects of hazards (see also P95 & P96).

P75 - Qualification procedure to confirm performance under specified conditions (see also P90).

P76 - Monitoring and inspection is expected, and where this is not possible, then additional measures are expected in order to assure lifetime performance.

P77 - There should be no requirement for human action in the first 30 minutes following any requirement for protective system action.

P78 - Single failure principle (see also **T/AST/011**).

P79 - Redundancy is assumed to be needed to achieve high reliability unless the necessary reliability can be shown to be otherwise achieved. Reliability claims based on redundancy are limited by CMF and a *limit* of 10E-5 would be expected (see P81). In practice a less reliable value may be appropriate. P80 & P81 which refer to diversity and CMF respectively, and T/AST/030 & **T/AST/036** are also relevant.

2.4 It should be noted that many of these general principles have been written in broad terms to cover a range of engineering applications, thus some interpretation is necessary in developing the guidance for individual application. In some cases, such as human factors, reference has been made to the relevant principles in order to provide an awareness of the issues to be considered. The detailed assessment of the particular subject will of course be carried out by the appropriate assessment section.

2.5 In addition to the above, the following SAPs and TAGs may also provide pertinent advice :

categorisation, codes and standards (P82-P85) and **T/AST/008**

design data and models (P86-P89)

human factors (P91-P94) and T/AST/012

maintenance, inspection and testing (P97-P101) and **T/AST/009**

plant ageing (P102-P103) and T/AST/016

reliability (P68 & P114-P118), see also T/AST/030

protection systems **(Ref 4)**.

3. Relationship to licence and other relevant legislation

3.1 The primary site licence conditions for which assessments of essential services are made are

LC 14 (Safety Documentation),

LC 24 (Operating Instructions), and

LC 27 (Safety mechanisms, devices and circuits).

3.2 Other licence conditions which may be relevant are

LC 15 (Periodic Review),

LC 19 (Construction/Installation of New Plant),

LC20 (Modification to Design of Plant Under Construction),

LC 22 (Modification or Experiment on Existing Plant),

LC 23 (Operating Rules),

LC 27 (Safety Mechanisms Devices and Circuits), and

LC 28 (Examination, inspection, maintenance and testing).

4. Advice to assessors

4.1 General Criteria

1) The assessor should confirm that the safety case clearly identifies all essential systems necessary to fulfil

the maximum requirement of the safety function required by the safety case. For each essential service so identified and provided **(P214)**, the safety case should define the necessary service capability and reliability, and define the time within which the service is to be provided. It should be confirmed that the service will be maintained for a sufficient period to bring the plant to a safe state and maintain it there until normal service supply is restored **(P216)**.

2) 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 within itself or the safety systems it supports such that its general availability to support safety functions is assured so far as is reasonably practicable. **P219** is directed particularly at this requirement to minimise the probability of the essential service being lost.

3) Where other facilities make use of any essential service, the means by which the essential function is preserved when 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 capability etc. and considered when assessing the adequacy of the service **(P217)**. 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 case should identify and tabulate (as above) the totality of the site essential service demands.

4) Particular attention should be given to reasonably foreseeable multiple or dependent faults which might give rise to the loss of a normal service and the back-up service. Specifically for electrical systems **(P221)**, the short term effects of loss of normal (off-site) and on-site AC electrical power should be addressed.

5) In assessing the adequacy of essential service

provision, the effects of adverse conditions and faults in the normal service or the essential service should be considered and the design shown to have incorporated adequate provision to ensure that the reliability of the service is not compromised. **(P218)**.

6) 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 requirements of the single failure principle **(P78, T/AST/011)** are met.

4.2 Sources of Supply

1) Each back-up or alternative source of supply should be considered, to confirm that each such source has the necessary capacity, availability and reliability to meet the maximum demands on it, and can provide that service for the necessary time **(P216)**.

2) Where any service is derived from a source external to the nuclear site, that service should where practicable also be obtainable from a back-up source on the site **(P215)**. Assessors should note that the terminology in the SAP is "where practicable", not "where reasonably practicable" to denote the expectation of a back up source. In the particular case where an essential service is only obtained from off the nuclear site, and thus may be outwith the direct control of the Licensee, particular attention should be given to the specification, availability and reliability, all of which should be of a similar standard as those for an on-site source. **(P220)**.

4.3 Specific Systems

1) As above, the safety submission from the licensee should clearly identify and define essential services necessary to ensure safety. The safety submission should also define the required performance of each essential service as well as demonstrating the adequacy of the capacity and capability of that service. It should also (preferably) define for each safety system, those essential supplies which are required, and identify the source. The list of typical essential services below should

not be assumed to be comprehensive. For each service, specific points are raised for assessment consideration.

2) Electrical supplies

i) Safety related plant and equipment normally derive their electrical supplies from the National Grid via the normal electrical distribution networks. On failure of these supplies, the safety related plant and equipment must be supplied from an alternative source. Emergency Supplies alternators (usually diesel or gas turbine driven) normally provide the bulk of these alternative AC supplies, but there will inevitably be a short term interruption to supply before these alternators come into service. Assessors should confirm that adequate provision is made for the necessary automatic alterations to the distribution networks, the starting of these generators and their connection to essential loads.

ii) For most of safety functions, interruption to supply is not tolerable. A number of options exist to provide uninterrupted supplies in such cases. These may typically be:

a) proprietary uninterruptable supplies systems consisting of self contained combinations of batteries (generally with integral on-load charging facilities), and motor generators or static alternators to provide AC supplies;

b) batteries, with off-load or on-load charging facilities, to provide DC supplies;

c) the arrangements to ensure that the capacity of such

batteries is adequate to maintain supplies until the essential electrical distribution is appropriately aligned.

The nature of the particular safety related plant or equipment will dictate the type of arrangement that is needed.

iii) Given the range of safety systems and the age spread of nuclear installations, it is beyond the scope of this guide to define the combinations which will need to be assessed, but typical examples are listed in the ensuing paragraphs.

iv) Interruptable AC supplies are 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.

v) Uninterruptable AC supplies are typically required for:

a) AC motors driving critical cooling pumps and critical ventilation systems, e.g. dissolver off-gas,

b) primary monitoring instrumentation such as criticality detectors, reactor instrumentation, radiation and contamination detection etc.,

c) electrical relays handling the unloading of normal supplies from the system to allow the essential electrical supplies to be brought into operation,

d) electrical relays used to trip and initiate electrical switchgear,

e) valve actuators required to isolate damaged sections of the plant and activate alternative cooling circuits, and

f) ventilation systems needed to maintain the quality of air in the control room environment and to remove contaminated air to suitable filter systems.

vi) DC supplies are generally required to support stand alone systems such as lighting, communications systems, and some smaller critical drives on older plants designed before the advent of reliable inverter packages.

vii) Adequate electrical analysis should have been carried out to ensure that the systems are capable of carrying out the demands that are placed upon them. These should include:

a) load schedule 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,

b) electrical fault analysis to ensure that the system can handle the expected fault currents under earth fault and short-circuit conditions,

c) voltage studies on dc systems to ensure that end of leg supplies are at a high enough voltage to operate the electrical plant and equipment,

and

d) fault protection discrimination studies.

3) Gas supplies

i) Gas supplies required for safety such as carbon dioxide, nitrogen, etc. are normally provided by routine deliveries to the site by road tankers. To provide an alternative supply on the site, it is necessary to ensure that the storage facilities are adequately sized to ensure 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.

ii) The storage facilities for these gases, and the design of the distribution system should be assessed as above under general criteria to confirm their capability and reliability using as a guide both the identified essential services SAPs and the other supporting SAPs.

iii) When assessing essential gas supplies, attention should be given to any requirements for steam or electrical supplies to vaporise or condition the gas before distribution and / or to the possibility of extreme temperature being experienced by the distribution system. The condition of the vacuum insulated vessels and associated equipment for maintaining the vacuum should also be examined. Pressure relief of insulated or vacuum vessels and associated vessels can lead to particular problems of embrittlement which may need special attention.

4) Water supplies

i) Supply of water to the site is typically via the townswater supplies from the local reservoir(s). 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, etc.) and minimum supply holdings justified and demonstrated as discussed in **para 4.3 3) i**).

ii) 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 and assessment similar to **para 4.3 3) ii**) above carried out.

iii) The provision of all water supplies defined as relevant to nuclear safety should be shown to be independent of any supplies required for fire fighting purposes.

iv) Essential cooling water supplies should be defined in the safety submission, and particular care should be taken to confirm that any essential service functions of any auxiliary cooling water systems are defined. These supplies should be available within a defined period, to meet the plant cooling requirements as specified in the safety submission.

v) 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.

5) Compressed air

i) This will normally be provided via a

compressor/storage vessel/distribution system(s). In some cases essential supply may be claimed as, or supported by, a central or distributed system of high pressure air bottles, or by cross connection to lower quality air systems, e.g. factory or general purpose air. The main considerations in this case are the failure of the air compressors, the supply pipework and the storage vessels as faults in this area can have widespread effects such as the generation of missiles. As with other essential services, it should therefore be ascertained that the capacity of the storage vessels is adequate to continue to supply the essential equipment (typically instrumentation) for the period defined in the fault studies, and that the quality of the air supply will not degrade the performance of the equipment. It should in particular be noted that derogation of quality of supply in respect of moisture or particulate content may have latent and / or long lasting detrimental effects on the reliability of instrumentation operated by compressed air.

ii) The storage facilities for these gases, and the design of the distribution system should be assessed as above under general criteria to confirm their capability and reliability using as a guide both the identified essential services SAPs and the other supporting SAPs. Consideration should also be given to the segregation and isolation of the normal and essential air systems to ensure that pressure hazards and random failures (leaks, non-return valves, etc.) do not degrade the system.

iii) When assessing compressed air supplies, attention should be given to the requirements for electrical and cooling water supplies to support the compressors.

6) Fuel

i) 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). As with compressed gases, normal supply of fuel (e.g. diesel) will be by means of routine tanker deliveries to on-site storage facilities. Although strictly outwith the requirements of this TAG, Ref 3 on Fire Protection is relevant to such facilities. The provision of an alternative on-site supply is a requirement to ensure that the capacity of the on-site storage of fuel is adequate to meet the fault study assumptions and minimum stock levels should be set, justified and monitored.

ii) Special attention should be paid to the fuel pipe/valve supply arrangements and to the storage tank segregation to ensure that a common mode fuel supply fault to the prime movers cannot occur. It should be noted that the control of the alignment of fuel lines to generators or steam plant has been a particular problem in the past and appropriate design provision should be included to control and if necessary monitor such alignments.

iii) Further attention should also be given to the manner in which tanker deliveries are arranged to ensure that no single fault, e.g. wet or dirty fuel, in any fuel delivery to the facility will cause a multiple failure of the prime movers. This is typically achieved by staggered delivery of fuel and the avoidance of cross transfers.

iv) The licensee should have suitable arrangements in place to ensure that the appropriate quality of fuel is delivered and maintained whilst in the storage tanks. The arrangements for monitoring the condition of

the storage tanks may also require to be assessed.

7) Lubricants etc.

i) Adequate lubrication of moving/rotating safety related plant and equipment should be considered by the assessor both from the design and maintenance viewpoints. For example when evaluating safety significant cooling circulating pumps, lubricated by a circulating oil system, diversity of oil supply as well as 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.

8) Steam raising supplies

i) Where there is an identified requirement for an essential steam raising supply (e.g. to vaporise CO_2) the arrangements for the boiler fuel supplies (for starting and running), boiler ignition, feedwater 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.

4.4 Equipment Qualification

1) The qualification basis of the essential services should be quoted and demonstrated to encompass all anticipated fault and environmental conditions. Further advice is given in **T/AST/008**. In particular, the basis of seismic qualification should either be stated in the safety case, or any absence of such qualification noted and

justified.

4.5 Life Cycle Requirements

1) The SAPs include a final section which addresses the need to identify the actions necessary to ensure that a high standard of safety will be maintained throughout the various phases of the lifetime of the plant. The main points to be considered in respect of the essential services relate to maintenance, testing and plant operation.

2) The design of the services should take into account the ability to routinely maintain, test and monitor the plant throughout the lifetime of the station 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.

3) Effect of plant modifications

i) As the plant is operated and modified, changes will be made which will affect essential services. As such changes may have been considered in isolation, there should be provision for regular comprehensive review of the effects of modifications on the essential services and the demands placed on those services.

4) Operation of the plant

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

cabinets, valves, etc.) for the services should be considered.

References

1. Safety Assessment Principles for Nuclear Plants (HSE 1992).

2. IAEA Safety Guide No 50-SG-D7 (Rev 1): Emergency Power Systems at Nuclear Power Plants (1991).

3. IAEA Safety Guide No 50-SG-D2: Fire Protection in Nuclear Power Plants (1992).

4. IAEA Safety Guide No 50-SG-D3: Protection System and Related Features in Nuclear Power Plants (1980).

5. Refs. 2, 3 and 4 although current are soon to be revised