NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM		
TECHNICAL ASSESSMENT GUIDE **SAFETY CATEGORISATION AND EQUIPMENT QUALIFICATION**		**T/AST/008** ISSUE 001
Approved By: *R P Pape*	R P Pape	Issue Date: 2/10/00
Open Government Status: Fully Open		Review Date: 1/10/03

Contents

1. Purpose and scope

1.1 The Safety Assessment Principles [1] contain key engineering principles which address the need for all structures systems and components to be allocated a *safety categorisation (P69)*, and for a *qualification procedure (P75)* to be in place to provide assurance that all safety systems and safety related equipment will perform the required functions throughout their operational lives. This TAG provides more detailed guidance on the interpretation of these principles, also making reference to other related general principles, and the approach to be adopted when assessing older plant.

1.2 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 Categorisation, codes and standards

P69, P82, P83, P84 and P85.

2.2 Equipment qualification

P75 and P90.

2.3 Other principles which have been drawn upon to assist in the interpretation of the above include P97-101 (maintenance, inspection and testing), P76 (monitoring and inspecting) and P102 - 103 (plant ageing). The defence in depth approach to the design and operation of a nuclear plant requires the incorporation of conservatively designed features, to prevent the breach of any barriers to the release of radioactive materials to the environment, or mitigate the consequences of a breach (P65). It is therefore necessary to determine the safety function of all structures, systems and components, and to allocate to each a safety categorisation in accordance with principle P69 (paragraph 131).

2.4 When the categorisation has been established, this is then used as the basis for the selection of the appropriate design and construction standards (P83), maintenance and condition monitoring requirements (P97 etc) and equipment qualification (P75) requirements which provide assurance that the structures, systems and components will be capable of performing the required safety function, throughout their operational lives. The categorisation principle is also relevant for civil engineering considerations, and this is addressed in a separate guide [2].

2.5 The development of the design philosophy in many overseas nuclear power plants has led to two clearly identifiable categories. These are: safety classified, meaning all those structures, systems and components claimed to perform a safety function; and non-safety, meaning everything else. The "safety classified" category may also encompass specific safety class gradings, in particular for mechanical items [3,4,5], which have been developed on deterministic criteria to define three separate classes for which different design codes are permitted.

2.6 The UK, in common with some other countries, has recognised the benefit of introducing a third category, which, whilst not performing the highest level of safety function, nevertheless provides a significant contribution to safety by mitigating the effects of or reducing the frequency of accidents. This has therefore resulted in the introduction of an intermediate category of plant designated as category 2.

3. Relationship to licence and other relevant legislation

3.1 The primary licence conditions which would be of relevance in any assessment request involving safety categorisation and equipment qualification are:

LC14 - safety documentation

LC16 - site plan, designs and specification

LC17 - quality assurance

LC19 - construction or installation of new plant

LC20 - modification to design of plant under construction

LC22 - modification or experiment on existing plant.

3.2 It should also be noted that the following licence conditions may be involved, or implicated, because of plant lifetime considerations:

LC15 - periodic review

LC21 - commissioning

LC27 - safety mechanisms, devices and circuits

LC28 - examination, inspection, maintenance and testing.

4. Advice to assessors

4.1 Safety Categorisation

1) In order to establish the safety significance of the structures, systems and components of a nuclear plant, it is necessary to define, in broad terms, three categories. The placement into any one of the categories requires judgement with respect to the item's importance to safety, assisted by a knowledge of, for example, the claimed reliability from fault or PSA studies. Guidance is provided in terms of INES ratings for accident consequence on failure, though in applying this guidance due regard should be given to the subjectivity of such ratings. Categories are normally defined by the licensee, usually after discussion with NII in areas where there is doubt.

2) **Category 1** is defined as "any structure, system or component which forms a principal means of ensuring nuclear safety". These items are the most important to safety. "Principal means" of ensuring nuclear safety should include the following:

i. any item whose failure would lead directly to a beyond design basis event corresponding to an INES 5 or higher rating. This includes so called "incredibility of failure" items;

ii. any item or collection of items (including operator alerting systems) provided to terminate or mitigate any initiating fault within the design basis with potential for an INES 5 or higher event rating;

iii. any item that contributes to the operator's ability to diagnose faults or hazards with potential for an INES 5 or higher event rating;

iv. for an overseas design, any other item which has been designated as safety classified or equivalent in the country of origin.

3) **Category 2** is defined as "any structure, system or component which makes a significant contribution to nuclear safety". The definition of "significant contribution" should include any item which is not otherwise required to be category 1, but which:

i. is claimed to reduce the frequency of an initiating fault or hazard within the design basis with potential for an INES 3 or 4 event rating;

ii. includes any item or collection of items (including operator alerting systems) provided to terminate or mitigate any initiating fault within the design basis with potential for an INES 3 or 4 event rating;

iii. contributes to the operator's ability to diagnose faults or hazards with potential for an INES 3 or 4 event rating;

iv. may be claimed to mitigate the consequences of a beyond design basis severe accident, or to reduce its frequency.

4) **Category 3** is defined as "any other structure, system or component", i.e., that which is not in category 1 or 2, and where failure cannot lead to an event greater than an INES 2 rating.

5) The safety case should include a clear explanation of the design standards to be used, and a justification for their use. This should be based upon a categorisation method for all structures, systems and components. Principle P83 states that "all structures, systems and components should be designed, constructed and inspected to the highest standards commensurate with their safety categorisation". Where there is no appropriate code or standard, P84 allows alternative methods to be adopted. It should be noted that where practicable, combining of different codes and standards should be avoided. Where this is unavoidable, a thorough justification of the methodology should be presented. In line with P 85, all standards, codes and alternative methodologies should adequately take into account degradation effects that can be reasonably expected to affect the items in question during their operational life. Where these effects are not fully understood, or where the initial state of the item is not determinable, conservatisms should be introduced into the analysis. The appropriate standards as defined in principle 83, together with their interpretation are as follows:

6) **Category 1** - Conservative design and construction standards should be adopted for this, the highest category. For some items (such as those whose failure would lead directly to an event beyond the design basis) the special case procedure (P70) may need to be used. Structures, systems and components within this category are referred to as "*safety classified*".

i. For mechanical items, acceptable conservative design and construction standards will be taken to include the ASME safety class 1, 2 or 3 [5] or equivalent, and for electrical items the appropriate standard is the US IEEE Class 1E [6] or equivalent. These are quoted as the reference standards since they include requirements for environmental testing which have not yet been incorporated into UK standards, although licensees would be expected to include such requirements in their own specifications. There are, however, continuing developments in international standards, for example through the ISO (International Standards Organisation) and the use of such standards may be accepted, provided equivalence with the above standard can be demonstrated.

ii. Items in this category should be included in the maintenance, inspection and testing schedule and be subjected to a rigorous maintenance and inspection regime which should include condition monitoring wherever reasonably practicable.

iii. The application of the special case procedure is addressed in other assessment guides and will not be considered further in this document.

iv. The standard of QA applied should follow the best international nuclear practice. Current acceptable standards would include, for example the IAEA Code [7] and British Standard 5882 [8], or the appropriate part of ISO 9000 series (further information is given in T/AST/40).

7) **Category 2 -** appropriate national or international codes or standards should be adopted, with particular consideration being given to demonstrating the ability of the item to perform the required safety function.

i. Items which are placed into this category may be constructed to similar standards to those for safety classified plant, in particular where the item may have some potentially adverse effect on category 1 plant.

ii. For other category 2 items national or international standards can be accepted but may need to be augmented by additional environmental testing to provide assurance that it will carry out its required function under the specified conditions.

iii. Rigorous QA standards should be applied for this category. As a minimum this should follow the best international commercial practice [9] with particular attention being given to the ability to perform the safety duty under the specified conditions.

8) Periodic checking of the item's ability to perform its required duty is also required by inclusion on the maintenance inspection and test schedule (P97).

9) **Category 3 -** normal industrial standards are acceptable for items within this category.

10) **Category S -** A further category of plant, "S" (seismic by association), has been established. It is used for categorising plant which, although itself having no safety significance, might seriously affect the operation of category 1 or 2 plant if it were to fail structurally during a seismic event. Examples of these are walls, pipework etc. This type of plant would be required to be seismically qualified to demonstrate that the risk from it was acceptable.

11) The categorisation of plant is a difficult process. It is significantly dependent upon the safety function that the plant is required to support. The same plant may occur in a number of places where it may be differently categorised. **Appendix 1** has been provided to demonstrate some examples of the process as it was carried out for Sizewell B. It should be noted that these are not definitive and are only justified within the Sizewell B context. Consideration must still be given to the local safety dependency.

4.2 Equipment qualification

1) The purpose of equipment qualification is to establish fitness for purpose for all specified conditions to which the equipment may be subjected, and to determine the period for which it must achieve such fitness, this period being its qualified life.

2) In order to establish the requirements for equipment qualification, several SAPs need to be drawn together. Principle P75 states that "a qualification procedure should be in place....", and this is further expanded in principle P90 which addresses the need for the "recording and retrieval of lifetime data." Principle P72 refers to the methodology whereby "external and internal hazards which could affect the safety of the plant should be identified ." Finally, principle P97 states that ".... components should, where practicable, be type tested under conditions at least equal to the most severe expected ....."; and ageing considerations are defined in principles P102 and P103. The aspects of the above principles which have implications for QA (e.g. lifetime records) are not discussed further in this document, but the following points should be taken into consideration when judging the adequacy of the equipment qualification programme.

3) Environmental conditions

i. The environments, during normal and fault conditions, which the item of equipment is expected to operate in, or may have to survive, should be detailed together with the period of time for which the equipment is required to operate. It should be clearly established whether the item is expected to operate through the environmental influence or just to operate after the event.

ii. Environmental factors include:

   a. Temperature

   b. Pressure

   c. Humidity

   d. Radiation

   e. Spray from chemicals, steam, water, etc..

   f. Seismic forces

   g. Vibration

   h. Electrical, magnetic, and electromagnetic effects e.g.. radio-frequency interference (See Assessment Guide **T/AST/015**)

   i. Flooding / immersion / precipitation / snow, rain, fog, etc

4) Operating conditions

i. All system parameter variations and where applicable, motive power parameter variations, e.g.. high / low voltage, air pressure, steam temperature / pressure, etc.., over which the required performance is to be achieved should be defined.

5) Qualification method

i. Equipment qualification may be accomplished by type testing, or in part by analysis depending upon the particular situation and the practicalities of the testing. In some cases, it may be possible to call upon actual seismic performance data for certain systems and structures, especially on existing plant. The main points to consider for each method are discussed in the following paragraphs.

6) Type testing

i. Type testing should be regarded as the preferred method. Exceptions should only be considered where such testing is not reasonably practicable.

ii. When this qualification method is used the limitations of conditions simulation, and the validity of data extrapolation should be clearly identified and taken into account. The sequence of testing and combinations of test conditions should be examined to ensure that synergistic effects have been addressed.

iii. The test procedure should include provisions to verify that adequate margins (the greater the safety significance the greater the required confidence in the margin) exist between the most severe specified service conditions of the plant and the conditions used in type testing; to account for normal variations in commercial production of equipment and reasonable errors in defining satisfactory performance.

7) Operating experience

i. Operating experience or experience data may only be used when it can be clearly demonstrated that the experience cited is applicable to the functional requirements and conditions for which the equipment is to be qualified. It is not normally accepted for new plant, and its main application is for the evaluation of the seismic capability of existing plants which were not originally qualified for a seismic event. Where experience data is used to qualify plant, it should be supported by a rigorous demonstration of the similarity of the plant to be qualified to that used to generate the database.

8) Analysis

i. Qualification by analysis is not generally acceptable as the sole method of qualification. When used it should include justification of methods, theories and assumptions. For complex items a combination of analysis and specific type testing may be accepted, subject to a satisfactory case being made.

9) Ageing

i. Where the qualification method either indicates a qualified life less than the anticipated installed life, or is unable to adequately predict the qualified life, then an acceptable on-going qualification programme is required. This may entail:

    a. Ageing and testing of identical items during the qualified life of the installed equipment.

    b. Additional, or sacrificial, equipment being installed in locations where service conditions equal or exceed those of the equipment under review. This could then be removed before the end of the qualified life period and type tested to determine additional qualified life.

ii. Other methods with proper justification may be found equivalent. Should the above methods demonstrate that the qualified life is less than the required life, the process of on-going qualification should continue or an equipment replacement programme should be instituted.

iii. The effects of ageing upon performance should be examined, when assessing the adequacy of test procedures.

10) Performance specification

i. The performance specification for normal and fault situations should be defined.

ii. Where safety systems may be employed either to perform more than one safety function or in several places for separate safety uses, then a separate set of performance requirements should be defined for each function or use unless it can be demonstrated that conditions for one function or use are bounding.

iii. The conditions within which the equipment is capable of operating, including both normal conditions and degraded state conditions (where relevant) should be defined.

iv. The qualified life of the equipment should be defined together with the requirements for preventive or other appropriate maintenance together with condition monitoring for assuring a qualified life. (Note:- Qualified life is the period of time which satisfactory performance can be demonstrated for a specific set of service conditions.)

v. Special care is needed to qualify equipment that is required to survive accident conditions (eg post-accident monitoring systems). The specification should require the equipment performance to exceed the worst case combination of conditions that the accident can expose it to.

11) Application to existing plant

i. The development of this guide has been based upon precedents established primarily from the assessment of Sizewell 'B', and also other recent new construction, including chemical plant. However, a significant proportion of assessment is of projects such as reactor and nuclear chemical plant periodic safety reviews, and licensing of existing installations (MoD establishments), etc. The balance in design between material quality and certification, analysis methods and accuracy, construction quality etc, will be different from today's. Therefore, these plants may not completely satisfy the more rigorous standards of today.

ii. For such plant, the assessor should still take into account the general guidance given above, in order to establish a confidence level in the adequacy of the original standards to which the plant was built, and to identify potential weaknesses in the plant's response to the range of normal and fault conditions to which it may be exposed. Any major modification work carried out on the plant should be assessed to determine the potential it may have for affecting the capability of existing qualified equipment.

iii. Operating experience feedback should form an essential part of any justification for the continued operation of plant for which the construction or manufacturing standards fall short of today's standards. One typical approach which should be examined is ageing and trending analysis, whereby the results of plant failures, condition monitoring, routine maintenance and testing are regularly analysed in order to help predict whether an item is about to fail, or to establish a worsening reliability for a family of items.

iv. Older plant was not generally qualified against seismic events. The use of experience data is therefore frequently claimed as a justification for items which may have to provide a safety function following an earthquake. Whilst this has been accepted as a method of providing confidence, it is important that the following questions are addressed when assessing the claim:

   a. does the estimated spectrum of seismic motion which the relevant plant in the database successfully survived bound the design spectrum for the item being qualified?

   b. has the item been shown to be similar to plant in the relevant category of the database, and that there are no features which may compromise its seismic ruggedness?

   c. has the anchorage of the plant been shown to be adequate in terms of strength, rigidity and installation?

v. If the answer to any of the above questions is no, then the assessor should consider that further plant improvements may be required. In addition:

   a. potential seismic interactions with other nearby equipment should also be addressed for effects such as falling debris (Category S).

vi. In general, electrical relays should be qualified separately, or a case made that maloperation of the relay during a seismic event will not lead to a more dangerous situation.

vii. Where there is considerable doubt that an item would perform its safety function in specified fault conditions, then the assessor should consider whether some additional protection of that particular feature needs to be provided. An example of this would be in the case of a potential exposure to high temperature (e.g. steam release) where additional physical protection of the item may be needed to protect it against exceeding its claimed limiting operating temperature. Alternative means of achieving the required safety function should also be sought.

Appendix 1 - Examples of categorisation process

A1.1 The following examples have been provided to demonstrate some results of the categorisation process as carried out at Sizewell B. They are neither exhaustive nor definitive. They do however suggest categories that have been considered suitable for plant in this particular situation.

Plant Item	Category	Supporting information.

Steam Generator primary side shell, secondary side shell, tubes, supports, divider plate, feedwater ring.	1	Failure of these steam generator components could lead to a LOCA and therefore have a significant effect on nuclear safety.
Steam generator internal structures	2	Failure of these components could reduce the effectiveness of reactor cooling but would not result in a LOCA. These do however carry a seismic category "S".
Pressuriser shell, heater sheaths, safety valves	1	Failure of these components could lead to a LOCA and therefore have a significant effect on nuclear safety.
Pressuriser heater elements	2	These are contained within the heater sheaths and so would not result in a LOCA. Their failure could however result in a reduction in performance of the Pressuriser and thus affect nuclear safety.
Main Control Room control panels	1	Primary reactor safety system.
Safety information display system	1	Primary reactor safety system.
High integrity control system	1	Primary reactor safety system.
Main Control Room operator and supervisors desk	3	Indication only. Not safety systems.
Distributed computer system	2	Will affect the operators ability to judge the state of the plant but is not part of the primary control and safety systems.
Control rod drive systems.	2	This will inhibit the operators ability to move the control rods. However, separate safety features force the control rods into the reactor to ensure ultimate nuclear safety.
Essential electrical system switchgear, batteries, chargers, inverters, cabling.	1	Needed to provide electrical power to nuclear safety plant. Will directly affect the nuclear safety systems.
11-3.3kv transformers.	2	Not actually part of the essential supplies system but used to energise these systems under normal circumstances. Malfunction of these systems unnecessarily loads the essential on site electrical power sources.
Non essential cables	3	These cables have no bearing on nuclear safety
Fuel handling transfer tube closure	1	Could allow a nuclear release from the tube.
New fuel elevator	3	damage to new fuel will not result in a radiological release.

References

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

2. T/AST/017 - Structural Integrity: Civil Engineering Aspects

3. ANSI, Nuclear Safety Criteria for the Design of Stationary PWR Plants, ANSI/ANS-51.1 - 1983

4. Safety Functions and Component Classification for BWR, PWR and PTR - A Safety Guide - IAEA Safety Series No, 50-SG-D1 (1979)

5. American Society of Mechanical Engineers, Boiler and Pressure Vessel Code Sections I-III

6. IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Std 323-1983

7. Code on the Safety of Nuclear Power Plants - Quality Assurance - IAEA Safety Series 50-C-Q (Rev 2) 1995

8. A Total Quality Assurance Programme for Nuclear Installations (1990) (British Standards BS 5882)

9. Quality Systems (1994) (ISO 9000 series)