

## Design safety assurance

**T/AST/057**

<b>Date issued:</b> 2007-16-04	<b>OG Status:</b> Fully open
<b>Review date:</b> 2010-16-04	<b>Author Unit/Section:</b> Mark Gabbott

## 1. Purpose and Scope

1.1 This Technical Assessment Guide (TAG) discusses NII's approach to the assessment of design arrangements and processes for nuclear facilities, and how safety is integrated into the design production process. In particular the design arrangements should demonstrate how integration with procurement, site construction/installation and final commissioning is achieved, leading into operations and associated maintenance and inspection, as well as the safety case development process. This TAG does not specifically address a single Licence Condition or group of Safety Assessment Principles, but concerns an area of activity which is of regulatory interest.

1.2 It should be noted that the Nuclear Installations Act 1965 (as amended) makes specific reference to design as an activity which may be subject to licence conditions.

1.3 Licence Condition 14 requires that the licensee "shall make and implement adequate arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation."

1.4 Licence Condition 19 requires that "Where the licensee proposes to construct or install any new plant which may affect safety the licensee shall make and implement adequate arrangements to control the construction or installation."

1.5 Licence Condition 20 requires that "The licensee shall ensure that no modification to the design which may affect safety is made to any plant during the period of construction except in accordance with adequate arrangements made and implemented by the licensee for that purpose."

1.6 Licence Condition 21 requires that "The licensee shall make and implement adequate arrangements for the commissioning of any plant or process which may affect safety."

1.7 Licence Condition 22 requires that "The licensee shall make and implement adequate arrangements to control any modification or experiment carried out on any part of the existing plant or processes which may affect safety."

1.8 This TAG contains general guidance to advise and inform NII Inspectors in the exercise of their professional regulatory judgement. This document is not intended to provide detailed guidance on the design process for nuclear facilities, but is produced to highlight certain key areas for consideration as part of an assessment process.

1.9 It is therefore essential that comprehensive reference is made to the HSE's Safety Assessment Principles (SAPs) for Nuclear Facilities and other TAGs when assessing such design arrangements and processes. References to the 2006 Edition of the SAPs and the January 2007 WENRA Reactor Safety Reference Levels are included in the text of this document.

1.10 Comments on this guide, and suggestions for future revisions, should be recorded on the appropriate registry file.

## **2. Relationship to licence conditions**

2.1 The following licence conditions have relevance in terms of design safety assurance:

- LC6 Documents, Records, Authorities and Certificates
- LC12 Duly Authorised and other Suitably Qualified and Experienced Persons
- LC14 Safety Documentation
- LC15 Periodic Review
- LC17 Quality Assurance
- LC19 Construction or Installation of New Plant
- LC20 Modification to Design of Plant Under Construction
- LC21 Commissioning
- LC22 Modification or Experiment on Existing Plant
- LC23 Operating Rules
- LC24 Operating Instructions
- LC25 Operational Records
- LC27 Safety Mechanisms, Devices and Circuits
- LC28 Examination, Inspection, Maintenance and Testing
- LC29 Duty to carry out Tests, Inspections and Examinations
- LC34 Leakage and Escape of Radioactive Material and Radioactive Waste
- LC35 Decommissioning
- LC36 Control of Organisational Change.

## **3. Legislation and regulatory interest**

3.1 The general duties under the Health and Safety at Work etc Act 1974 (HASAWA) impose statutory requirements as follows:

- 2 (1) It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.
- 3 (1) It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety.
- 6 (1) It shall be the duty of any person who designs, manufactures, imports or supplies any article for use at work or any article of fairground equipment –
  - (a) to ensure, so far as is reasonably practicable, that the article is so designed and constructed that it will be safe and without risks to health at all times when it is being set, used, cleaned or maintained by a person at work;

In addition, the Construction (Design and Management) Regulations 1994 place duties on designers to take due recognition of health and safety in the design process. The Ionising Radiations Regulations 1999 also make specific reference to engineering controls and design features as the primary means of restricting exposure to ionising radiation. Other regulations under the HASAWA also impose duties on designers for specified engineering features. Environmental Legislation, Security Legislation and International Treaties also impose legal duties on designers.

3.2 It should be recognised that design organisations may not be licensees themselves, but should be under the control of the appropriate licensee acting as an Intelligent Customer. Nevertheless, the statutory legislation noted above, plus the licence conditions themselves, provide the NII with the necessary vires to regulate design activity, through coordination with the licensee.

3.3 This regulatory interest equally applies to the early stages of the design process, at the optioneering stages. However, a clear balance needs to be struck between the benefits of leverage which can be achieved by early guidance/intervention, and the potential negative, disruptive effects which can occur due to detailed questioning of early concepts. Furthermore, caution is necessary to ensure that an impression that a design has been approved is not given.

3.4 In particular, the NII should focus on standards and principles, the visibility of optioneering to demonstrate ALARP plus the adequacy of the design process and associated arrangements.

## **4. BMS guidance**

4.1 The assessor needs to be aware of NII's expectations more generally for Licensees' safety cases and how they are produced, which are set out elsewhere within other BMS Guidance documentation.

A number of other Technical Assessment Guides will be relevant to the subject of Design Safety Assurance and the assessor should review the latest available information on the BMS.

## **5. Advice to assessors**

### **Introduction**

5.1 This guide is concerned with the assessment of arrangements for the production of design for structures, systems and components for nuclear facilities. These arrangements should demonstrate that safety considerations are integral to the design process, and that the formal safety justification as evidenced by the relevant safety case, is fully coordinated with the design activity and should evolve in parallel.

5.2 The purpose of NII assessment of design safety assurance is to establish whether the design arrangements, including interfaces with procurement and construction/installation, leading into the operations and associated maintenance and inspection, are adequate to fulfil the required safety functions, and to establish that the hazards created by such arrangements are both tolerable and ALARP, in compliance with legal requirements.

## **Engineering background**

5.3 All structures, systems and components are specified and designed to provide a required engineering functionality. This functionality will have an influence on safety and so requires an appropriate safety categorisation to be assigned. This categorisation (or grading) will affect the design methods and standards, material selection, procurement process, fabrication and installation inspections as well as maintenance requirements and in service inspections.

5.4 In any engineering process, the resource available (whether it be in time or budget) relating to required activities such as design is always limited. It is therefore appropriate that such resource is targeted at areas which have the greatest potential for danger. This is the basis for all engineering safety categorisation systems.

## **Design requirements and regulations**

5.5 Design requirements arise generally for the following reasons:

- The licensee wishes to design, construct, install and commission a facility on a new site, or within an existing site. Licence conditions 19, 20 and 21 are specifically applicable to this scenario, as well as the requirements for site licensing for new sites.
- The licensee wishes to undertake a modification to an existing facility. Licence condition 22 is specifically applicable to this scenario.
- The licensee is conducting an assessment of structures, systems and components for a periodic safety review. Licence condition 15 is specifically applicable to this scenario.
- The licensee wishes to decommission a facility. Licence condition 35 is specifically applicable to this scenario.

Early regulatory involvement in the design process can provide assurance that the necessary arrangements are in place to ensure safety, as well as provide preliminary indications as to whether the final design solution will be satisfactory.

For new build it may be a vendor who is responsible for design development and control prior to the appointment of a licensee. Under these circumstances the vendor's design management process may still be subject to regulatory review, and a regulatory strategy should be developed for this which should take cognisance of the guidance provided in this document.

## **Design process**

5.6 The design process can be a complex undertaking, involving parties from different disciplines who contribute to the overall design product. This design process will vary between disciplines, but issues of key importance are listed as follows, with discussion in the subsequent paragraphs:

- Design Phases (5.7)
- Hazard Identification (5.8)
- Optioneering (5.9)
- Safety Functional Requirements and Design Parameters (5.10)
- Design Planning and Organisation (5.11)
- Design Standards (5.12)
- Design Verification and Validation (5.13)
- The Interface with Procurement (5.14)
- The Interfaces between Design Disciplines (5.15)
- Information Control and Document Management (5.16)
- Change Control (5.17)
- Competency (5.18)
- The Interface with Construction/Installation (5.19)
- The Interface with Commissioning (5.20)
- The Interface with Maintenance and Inspection (5.21)
- Safety Case Production and Interface (5.22)
- Design Review (5.23)
- Design Instructions (5.24)
- Fault Recording and Corrective Action Systems (5.25)
- Intelligent Customer and Design Authority (5.26)
- Human Factors (5.27)
- Design Quality Assurance (5.28)
- Design for Decommissioning (5.29)

## **5.7 Design Phases**

A well structured design process is the starting point for a successful design output. The design process should clearly integrate with the safety case production process. There must be a regular two way interaction with the safety case authors such that the designers recognise the need for risks associated with design solutions to be

ALARP, with clear evidence of optioneering. Early input from facility operators and maintenance organisations is also necessary. It is important to recognise the safety significance of elements of the design to determine the rigour of the safety review. It must be recognised that the design process is generally iterative, and the key requirement is that the risk associated with the overall functional solution is ALARP. Attempts to justify individual 'building blocks' of the overall design solution to ALARP criteria may not be helpful. The safety case authors need to keep abreast of the developing design solutions and associated detail to ensure that the claims made in the safety case remain valid and accurate. A typical design process and integrated safety justification should proceed as follows:

- Inception and initial brief
- Feasibility studies and optioneering
- Conceptual design → Preliminary Safety Report
- Scheme design → Design freeze
- Detailed design → Design freeze → Pre Construction Safety Report

It is necessary that key research and development outputs are available at an early stage in the process in order to allow the design to evolve in a logical progression.

The concept of design freeze is an important control tool in the design process, although it should be recognised that it does not, and should not impose absolute constraints on changes beyond this point. However, any such changes to frozen information should be formally justified and the implications assessed, particularly from a safety perspective, and thoroughly integrated into the modified design if the change is adopted. The degree of rigour required in the assessment of proposed changes and the associated implementation should be commensurate with their associated safety significance.

It should be noted in the above description that when the Pre Construction Safety Report is produced, the detailed design would generally be 'frozen', making changes difficult from a time and cost perspective. This reinforces the need for early regulatory interest in the design process. It is essential that the regulator is made aware of design changes subsequent to the issue of a licence instrument, as part of the regulatory process.

The design process will also integrate into the overall project management process and project sanctioning process. A number of project 'gates' may need to be successfully negotiated for the project to proceed, requiring specific design and safety case deliverables. Continuity of design resource may be an issue as a result of this process.

The design process should also incorporate features known to promote high reliability within organisational due processes, such as diversity and redundancy.

## **5.8 Hazard Identification**

Early hazard identification is an important part of design safety assurance and can utilise many different inductive and deductive techniques that are undertaken at appropriate project design stages. One standard format is a 'structured brainstorm' to identify hazards, followed by a risk assessment process to quantify the worst credible consequence and associated likelihood, usually expressed as a frequency for cumulative risk. Consequential risks, after the application of safeguards, are then assessed and determined to be either intolerable, within the ALARP region, or in the broadly acceptable region. It is important that identified safeguards, plus other measures subsequently developed following the hazard identification process are recorded and tracked through to conclusion, to ensure adequate implementation. A hazard schedule, which should be treated as a live document, is generally a good way to achieve this.

Fundamentally hazards should be eliminated and reduced by design where practicable, and most benefit in this respect is usually achieved at the early conceptual design stage.

It should be recognised however that although beneficial, document based hazard identification studies are limited in that they sometimes fail to recognise complex interactions between structures, systems and components. They should therefore be complemented by other methods of hazard identification such as virtual plant walkdowns, plus actual walkdowns during construction/installation and commissioning.

It is important that the hazard identification process provides a high degree of confidence that it can identify all credible postulated initiating events.

As the process develops, further risk assessments should be undertaken in an appropriate format to maintain the safety integrity of the design solutions.

The SAPs FA series (Fault analysis) and WENRA reference level E (Design Basis Envelope for Existing Reactors) are applicable to Hazard Identification.

## **5.9 Optioneering**

Optioneering is an essential early part of any design process, in order to ensure and demonstrate that solutions are ALARP. Optioneering is a very common project management technique, but can often focus on issues of cost, functionality and programme without specifically addressing safety. The legal requirement to satisfy the ALARP principle means that options related to safety should be addressed as part of the overall design solution. However, optioneering needs to be controlled from a design management perspective during the later detailed design phases in order that the activity can be focussed and moved forward, without each step being excessively challenged in detail. Furthermore, it should be recognised that optioneering at a microscopic level can be counterproductive and may not generally yield the best macroscopic solution, with a practical economy of effort.

The SAPs NT series (Numerical targets and legal limits) is applicable to Optioneering.

## **5.10 Safety Functional Requirements and Design Parameters**

Safety functional requirements are deterministic rules which are generated during the start of the design activity, which are considered necessary to ensure safety by identifying the specific safety requirements associated with structures, systems and components important to safety. These can cascade from high level safety requirements, to a larger number of lower level functional demands on individual structures, systems and components. The design should follow these requirements and update them as necessary as part of the process. These requirements should be confirmed during commissioning and then feed in to the operating rules and instructions as described by licence conditions 23 and 24.

Associated with safety functional requirements is the process whereby design parameters are established, to define the design duty of the structures, systems and components under consideration. In addition to categorising designs in accordance with SAPs, physical parameters should be established to define design duties, such as temperature, load combinations, damage and aging mechanisms, environmental considerations, design life considerations etc. This links to the overall consideration of equipment qualification.

The SAPs ECS series (Safety classification and standards) and WENRA reference level G (Safety Classification of Structures, Systems and Components) are applicable to Safety Functional Requirements and Design Parameters.

### **5.11 Design Planning and Organisation**

A well structured and resourced delivery plan/programme is a key part of a well executed design process. As such it leads directly to ensuring that safety is incorporated into the design output, by identifying safety process requirements, such as Hazops and safety case integration for example, as well as by facilitating a well organised, coordinated process, without which safety cannot be demonstrated and indeed may not be achieved. This plan should identify key inputs, formal design outputs, interdependencies, timescales plus resource requirements, generally in terms of design effort. The resource considerations should also address internal design skills, internal facilities, external skills and facilities (if consultants are used) plus the overall design organisation. A well structured, up to date and well communicated design organisation, evidenced through an organisation chart is a prerequisite for an effective process.

Design activities tend to be organised as either dedicated project teams, with personnel mixed from different technical disciplines, or as small project management/engineering groupings drawing on effort from functional teams, organised on a discipline basis. Often organisations operate with a mixture of both characteristics. Functional characteristics can bring significant safety assurance benefits in terms of providing collective functional knowledge, robust verification processes, collective competency and standardisation, but can have the disadvantage of discouraging good communication within the project leading to a 'silo' mentality.

The design programme should be integrated into the overall project and safety case programmes, with specific links to procurement and construction/installation to ensure an effective overall project is achieved. It is also important that suitable checks are in place for the review and questioning of input information, such that it is

not blindly incorporated into the design when it might be erroneous. This contributes to the defence in depth, which is an inherent feature of a highly reliable process.

Where design is undertaken at various levels of detail by different organisations, it is important to recognise that the Design Authority resides at the highest level, with overall responsibility for the functionality of the completed design product. This role of Design Authority is closely related to the requirement for the licensee to act as an Intelligent Customer.

It is important that the licensee should participate in all interactions between external design organisations and the NII, in order to ensure that the licensee develops and maintains this Intelligent Customer capability.

The design facility makes a significant contribution to an effective design process, and support resource in terms of personnel and equipment are important factors. Access to technical information is also very important, including availability of historical information.

Overall design resource numbers, as well as continuity, turnover, training and morale are significant issues in terms of design safety assurance. Training is a particularly important issue, and should cover not only introduction to new issues, but refresher training to maintain the 'conscious competence' mode of operation. Training should also cover physical appreciation of the designed structures, systems and components, and application within the intended facility.

The SAPs MS series (Leadership and management for safety) and WENRA reference level B (Operating Organisation) are applicable to Design Planning and Organisation.

## **5.12 Design Standards**

Establishing appropriate technical standards to underpin the design process is an essential early activity, which clearly has significant safety implications. A range of standards exists for nuclear design application, including IAEA standards, International, European and British standards as well as in house developed standards, (some with accepted general application with the UK nuclear industry). It is important that the design organisations have an up to date knowledge of the range of available standards, and are able to demonstrate a mature selection process for the specific design application. Selected standards must be effectively communicated within the design organisation, with training requirements identified and implemented as necessary. Changes to standards must also be effectively assessed, communicated and implemented, (although a design standards freeze may also be put in place).

The SAPs ECS series (Safety classification and standards) and WENRA reference level C (Quality Management) are applicable to Design Standards.

## **5.13 Design Verification and Validation**

Design verification is the process whereby each stage of the design is confirmed as correct against the requirements from the previous stage. This generally entails a

process of checking and approval. Two standard checking methods are usually applied, either a direct check of the calculation or design method, following the original philosophy, or alternatively a check by a parallel method or calculation. Generally the parallel method provides for a higher level of assurance, preventing a purely arithmetical check being undertaken for example, on what may be an erroneous philosophy. However, a parallel check does not check intermediate results in detail and so caution must be applied if these values are subsequently used. A complementary method of verification is by comparison with existing, proven design, although if this is used as the sole method of verification then the process must be extremely rigorous. The assurance of design verification can be categorised by assigning a checking category level, ranging from checks within the originating design teams, to independent checks undertaken by external organisations.

The hierarchy of verification is generally undertaken in a three tier structure, with an originator, checker and approver. The function of the approver from a verification perspective is to confirm there are no obvious errors, to ensure that the design output is consistent with other design elements, and to confirm the competency of the originator and checker and that the correct level of checking has been applied. Further tiers in the verification process can be counterproductive in diluting the level of individual responsibility and ownership. Notwithstanding the above, a culture of self verification, i.e. 'checking your own work', is evident in the most effective design organisations.

Design validation ensures that the overall intent of the design is achieved, and prevents failure of this objective by incremental deviation or dilution. This is achieved by a combination of independent technical assessment, peer review, design review, staged testing and commissioning plus operating trials.

Where software applications are used in the design process, rigorous software validation requirements must be in force, including for well structured version control. Design packages can be bought in externally or developed internally, using a range of software platforms, but the fundamental validation requirements are unchanged. Where commercial design software is used, it may be appropriate to run separate design codes as a form of validation. Challenges to the safety assurance of the design process can readily evolve from the uncontrolled growth and use of small, bespoke software routines, which have not been formally validated or controlled. Software should only be used for analyses within the bounds of its specified application and associated validation, and the results subjected to sanity checks by simplified calculations as necessary.

#### **5.14 The Interface with Procurement**

The interface with procurement is key to ensuring that the delivered structures, systems and components match the design intent. This requires robust systems for identifying products and materials in the first instance, and inspection systems to ensure that the material specified is correctly delivered by the supplier. Inspection systems are also required to verify the engineering functionality and can include type tests, batch sample tests plus routine tests (including proof tests). Tests can be undertaken at the factory (Factory Acceptable Tests, FATs) and on site (Site Acceptance Tests, SATs), as well as suitable tests on civil structures during the

construction phases (e.g. concrete cube tests). Tests may be destructive or non destructive, and samples from the destructive process should be fully destroyed to prevent inadvertent re-use. It is very important that such tests are well designed such that they mimic as closely as practicable the duties imposed on the structures, systems and components on which the design has been based, and meet specified standards as necessary. It should also be noted that there is considerable scope for misunderstanding regarding terminology associated with testing, and the specifications and arrangements for testing should be given a commensurate degree of technical effort to prevent this, in addition to quality assurance requirements.

Arrangements are also required to ensure that non conformances in respect of equipment and materials are adequately assessed and sentenced as appropriate. These arrangements should ensure that the potential non conformance is adequately recognised, categorised in terms of its safety significance, assessed at the correct level of technical competence and the resulting sentencing adequately implemented. The aggregate of a series of non conformances should also be captured within the process, both as evidence of potential systemic process problems, as well as identifying the cumulative effect on safety.

The SAPs EQU series (Equipment qualification) and WENRA reference level C (Quality Management) are applicable to the Interface with Procurement.

### **5.15 The Interfaces between Design Disciplines**

The interfaces between design disciplines are important from a safety perspective, specifically where design covers multidisciplinary areas. Some form of interdisciplinary check would be a firm expectation as part of any design process. Furthermore, in addition to processes to control detailed interfaces, it is important that suitably competent engineers have an overview of the whole designed system to ensure key issues are not missed.

### **5.16 Information Control and Document Management**

Information control, configuration control and document management are critical requirements where large numbers of design documents are produced as part of the process. Licence condition 17 requires adequate arrangements to be made in respect of Quality Assurance, QA. Licence condition 6 also requires adequate records to be made in respect of compliance to any licence condition. Documentation, whether in hard copy or electronic format is the fundamental output of any design process and a significant effort is required to ensure that such information is clear, comprehensive and unambiguous. The following issues are relevant to this subject from a safety perspective:

- Document identification
- Version control
- Presentation format including use of colours
- Projection methods and orientation

- Terminology
- Symbols
- Distribution
- Retention and availability of access to lifetime records
- Production of 'as fitted/as built' records

WENRA reference level C (Quality Management) is applicable to the issue of Information Control and Document Management.

### 5.17 Change Control

The management of change is a key part of the design process, from the early stages when the process may still be highly iterative, to the later stages where the volume of design information may be substantial. An understanding of the way in which the design information is structured or configured is also important in recognising the practical way that agreed changes should be implemented through the design system. The general principles of design change control and associated configuration management are as follows:

- Recognition of change
- Understanding the safety impact of change
- Agreement of change at the correct authority level
- Controlled implementation and communication of change
- Update of necessary documentation

As the design matures, agreement and authorisation of change is generally undertaken at more senior levels within the organisation. Once the procurement and construction cycles have commenced, the impact of potential changes from the design process are greatly magnified, as are the difficulties in correctly implementing such changes that are agreed. However, a mindset which automatically resists change due to its inherent difficulty will have a negative effect on safety assurance by the possibility of failing to recognise and sentence changes which are required.

The potential impact on safety can be substantial due to incorrect management of changes, which are consequently inadequately conceived and/or executed.

### 5.18 Competency

Licence condition 12 requires that only Suitably Qualified and Experienced Persons, (SQEPs), should perform any duties that may affect safety. This requirement also affects designers and so the design resource should be subject to a competency management system. This system should recognise the skills, technical discipline and experience of the designers and design management should ensure that activities are only undertaken by suitably qualified and experienced personnel.

WENRA reference level B (Operating Organisation) is applicable to the issue of Competency.

### **5.19 The Interface with Construction/Installation**

The design process should clearly link to the construction/installation process, such that adequate information is provided to the construction teams, and a process should be established whereby queries raised by these teams can be fed back and assessed by the designers. The use of field engineers with design office experience is recommended to fulfil this interface function. Recognition of changes requiring design review is fundamental. Licence conditions 19 and 20 have particular relevance to this issue. Arrangements are necessary in this area to ensure that non conformances are recognised, assessed at the correct level and duly sentenced by a controlled process.

### **5.20 The Interface with Commissioning**

The design process should also link to the commissioning process, such that adequate information is provided to the commissioning teams, and a process should be established whereby queries raised by these teams can be fed back and assessed by the designers. The use of commissioning engineers with design office experience is recommended to fulfil this interface function, with suitable input from future operators as part of the process. Recognition of changes requiring design review is fundamental. Licence condition 21 has particular relevance to this issue. Arrangements are necessary in this area to ensure that non conformances are recognised, assessed at the correct level and duly sentenced by a controlled process.

The commissioning process should confirm the assumptions made and requirements identified through the design process.

The SAPs ECM series (Commissioning) is applicable to the Interface with Commissioning.

### **5.21 The Interface with Maintenance and Inspection**

The design process should identify the requirements for examination, inspection, maintenance and testing of structures, systems and components as necessary to assure their continued safe operation. Due regard should be made during the design process to visibility and accessibility of structures, systems and components to meet this requirement. Specific attention should also be paid to facilitate the replacement of items which are intended to be renewed within the design life of the overall facility. Licence condition 28 has particular relevance to this issue.

The SAPs EMT series (Maintenance, inspection and testing) and WENRA reference level K (Maintenance, In-service inspection and Functional Testing) are applicable to the Interface with Maintenance and Inspection.

### **5.22 Safety Case Production and Interface**

The design process must lead to production of safety documentation that achieves the necessary level of assurance and reference should be made to the relevant BMS guidance.

Generally the safety case format should follow the claim, evidence, argument logical justification chain, whereby the design process should seek to primarily provide evidence in terms of design information and parameters.

Where existing facilities are subject to upgrade programmes, then establishing a firm understanding of the present state of the facility and original design intent is an important input into the design and safety case production activities. Where this information is not readily available, this can be achieved as part of formalised engineering substantiation processes.

The SAPs SC series (Safety cases) and WENRA reference level N (Contents and updating of Safety Analysis Report) are applicable to Safety Case Production and Interface.

### **5.23 Design Review**

Design review is a core requirement of any quality management system. At suitable planned stages, formal reviews should be undertaken to confirm the validity of the design, to act as a forum for information transfer and to identify problem areas and to give direction to solutions. It is important that such reviews are given a high level of support and importance, with participation from procurement and construction/installation disciplines where practicable. Typically a design review should ensure the following:

- The requirements of the brief have been identified and are being met
- Appropriate design acceptance criteria have been established and are being met
- The safety justification process is integrated into the design process
- Correct design parameters have been established
- The design identifies appropriate materials and products
- Appropriate and referenced design documentation is being produced
- The design identifies suitable limits and conditions of operation and safety

### **5.24 Design Instructions**

Formal procedures should be in place to ensure that design instructions, including those issued to installation teams which are not captured by other suitable documents, are put in place. Such instructions are often generated from the need

for direction in advance of formal incorporation into other design generated documentation. Nevertheless, these instructions should be formally generated, verified as appropriate and adequately controlled and distributed. It would be expected that they be incorporated into other formal documentation at an appropriate stage.

### **5.25 Fault Recording and Corrective Action Systems**

Formal processes should be in place to ensure that design associated faults and potential improvements identified from procurement, construction, installation, commissioning plus final operation and maintenance are fed back to the designers for consideration. This process is sometimes termed a Fault Recording and Corrective Action System. This consideration should generally follow the following model:

- Record and understand the fault
- Identify what action is required for existing designs/materials/installations on the project
- Identify what action is required for future designs/materials/installations on the project
- Identify what changes to design processes may be necessary for the future in general

From an overall perspective, 'lessons learned' workshops can provide a valuable learning format to ensure that difficulties are minimised for the future. These workshops should also identify positive features, as well as areas for improvement, to ensure that good practice is repeated in the future.

WENRA reference level J (System for Investigation of Events and Operational Experience Feedback) is applicable to the issue of Fault Recording and Corrective Action Systems.

### **5.26 Intelligent Customer and Design Authority**

Where design is contracted out, it is important that the licensee retains the role of Intelligent Customer, so as to correctly specify the design requirements, monitor the design delivery process and validate the output. Retention of corporate knowledge is closely associated with this issue. The organisation which has overall responsibility for the design process and maintenance of the facility design knowledge is termed the Design Authority. This design knowledge should be retained in a form that is practically retrievable and understandable for the lifetime of the facility's operational and decommissioning periods. The licensee is responsible in this respect for ensuring that an adequate Design Authority exists to oversee and maintain the integrity of the design. This Design Authority does not always exist within the licensee, but in these cases the licensee needs to clearly demonstrate the attributes of an Intelligent Customer. This licensee responsibility includes maintaining the necessary engineering skills and knowledge, implementation of appropriate research, and dealing with intellectual property issues as necessary.

This role of Intelligent Customer extends to the use of third party design consultants where they are used by the non licensee design house, as well as the interfaces with procurement and construction/installation.

WENRA reference level C (Quality Management) is applicable to the issue of Intelligent Customer and Design Authority.

### **5.27 Human Factors**

Human factors is an important consideration for the design process. The designed structures, systems and components should pay due recognition to human factors in terms of installation, subsequent operation and maintenance. Designers can sometimes create assemblies which only 'work' in their final configuration, without due recognition of how they can be safely assembled or maintained. Furthermore, since the mindset is generally one of ensuring that configurations do successfully work, designers sometimes fail to question how they could be misused or fail, in terms of systematically assessing what could go wrong at a detailed level.

Human factors input should be made to the design process to ensure that demands on operators to operate the equipment, maintain it and respond to failures are adequately assessed. Physical as well as theoretical models can play an important part in linking the design concepts to human factors issues, in terms of the final configuration.

Where necessary, guidance should be sought from specialist human factors practitioners.

The SAPs EHF series (Human factors) is applicable to the issue of Human Factors.

### **5.28 Design Quality Assurance**

Design activities must be internally regulated by current and controlled quality assurance procedures which are accessible to all users. These procedures should be enforced by a visible internal auditing regime, with evidence of observations and corrective action requirements as appropriate. As with all quality assurance auditing processes, there should be evidence of effective action and close out of issues to demonstrate a robust process.

WENRA reference level C (Quality Management) is applicable to Design Quality Assurance.

### **5.29 Design for Decommissioning**

Design solutions should take due recognition of the need for future decommissioning of facilities and equipment. This may include the need to replace equipment which becomes life expired, within the overall facility design life, in addition to decommissioning the facility as a whole. It should be recognised that the attributes which may provide straightforward decommissioning may run counter to those which are necessary to ensure safety during the operational lifetime of the facility, e.g. seismic capability may require substantial structural engineering solutions, which are challenging to decommission. Recognition of the future requirement however at the

design stage will allow the optimum solution to be achieved, whilst ensuring safety at all stages. Licence condition 35 has specific relevance to this issue.

The SAPs DC series (Decommissioning) is applicable to the issue of Design for Decommissioning.

## **Summary**

5.30 This guidance has been produced to advise the reader of key elements within a design process for items important to safety, primarily for application within the nuclear environment.

The detailed features of the design process itself will vary between disciplines and projects, but this document addresses the key elements which should be present in an effective design organisation that produces design solutions that will be demonstrably safe. The elements can be sampled, assessed and inspected to the necessary degree of rigour, as part of the regulatory process, to provide assurance of nuclear safety.

## 1. Bibliography and Further Reading

- (1) Nuclear Installations Act 1965 (as amended)
- (2) Health and Safety at Work Act 1974
- (3) Construction (Design and Management) Regulations 1994
- (4) Ionising Radiations Regulations 1999
- (5) Health and Safety Executive – Nuclear Site Licence Conditions, HSE website
- (6) The Tolerability of Risk from Nuclear Power Stations, Revised 1992
- (7) Reducing risk, protecting people, HSE's decision-making process, 2001
- (8) Quality management systems – Requirements, BS EN ISO 9001:2000
- (9) Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Codes and Safety Guides Q1-Q14, Safety Series No 50-C/SG-Q, IAEA, Vienna 2001
- (10) Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series, Requirements, NS-R-1, Vienna 2000
- (11) Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide, NS-G-1.2, Vienna 2001
- (12) Design management systems, BS 7000
  - Part 1: Guide to managing product design
  - Part 2: Guide to managing the design of manufactured products
  - Part 3: Guide to managing design in construction
- (13) DOE Standard Configuration Management, US Department of Energy website, ref DOE-STD-1073-2003
- (14) Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, IAEA, 2003
- (15) The Regulation of Nuclear Installations in the UK, including Notes for Licence Applicants, Draft for Trial Use, HSE November 2005
- (16) Safety Assessment Principles for Nuclear Facilities, Health and Safety Executive, 2006 Edition
- (17) WENRA Reactor Safety Reference Levels, Western European Nuclear Regulators' Association, January 2007