|  |
| --- |
|  |
| ONR Technical Assessment Guide  Design Safety Assurance |



ONR Technical Assessment Guide

Design Safety Assurance

Authored by: Principal Inspector – Mechanical Engineering and Nuclear Safety Inspector – Mechanical Engineering

Approved by: Professional Lead – Mechanical Engineering

Professional Lead: Mechanical Engineering

Issue No.: 7

Publication Date: May-2023

Next Major Review Date: May-2027

Document Ref. No.: NS-TAST-GD-057

Record Ref. No.: 2020/139039

Table - Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 5 | Minor update to reference the Ionising Radiation Regulations 2017. |
| 6 | Updated review period |
| 7 | Minor update to references and document structure |

Contents

[1. Introduction 4](#_Toc134780914)

[2. Purpose and Scope 4](#_Toc134780915)

[3. Relationship to Licence Conditions and other Relevant Legislation 5](#_Toc134780916)

[4. Advice to Assessors 7](#_Toc134780917)

[5. Summary 21](#_Toc134780918)

[Bibliography and Further Reading 22](#_Toc134780919)

[References 23](#_Toc134780920)

[Glossary and Abbreviations 24](#_Toc134780921)

# Introduction

1. ONR has established its [Safety Assessment Principles](http://www.onr.org.uk/saps/saps2014.pdf) (SAPs) [1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities. These facilities may be operated by potential licensees, existing licensees, or other duty-holders. The SAP principles are supported by a set of guides. These guides further assist ONR’s inspectors in their technical assessment work to support making regulatory judgements and decisions. This technical assessment guide (TAG) is one of these guides.

# Purpose and Scope

1. This TAG discusses ONR’s approach when looking at the suitability of the design arrangements and processes for nuclear facilities. It also looks at how safety is integrated into the design production process. In particular, the licensees design arrangements should show they sufficiently align with the following activities:

* procurement;
* construction;
* installation,
* commissioning,
* operation,
* maintenance,
* inspection; and
* the safety case development process.

1. This TAG contains general guidance and advice. It aims to inform ONR Inspectors when applying their professional regulatory judgement. This document does not provide detailed guidance on the design process for nuclear facilities. Its purpose is to highlight certain key areas for sampled assessment.
2. This TAG focuses on ensuring:

* the standards and principles are achieved;
* the optioneering is visible to help show that risks have been reduced ALARP[[1]](#footnote-2); and the design process and arrangements are adequate.

# Relationship to Licence Conditions and other Relevant Legislation

1. ONR’s inspectors should recognise that the Nuclear Installations Act 1965 (as amended) references design as an activity. This activity may be subject to licence conditions.

## Licence Conditions

1. The following licence conditions (LCs) are of principal relevance to design safety assurance:

* LC 6 - Documents, Records, Authorities and Certificates
* LC 14 - Safety Documentation
* LC 15 - Periodic Review
* LC 17 - Quality Assurance
* LC 19 - Construction or Installation of New Plant
* LC 20 - Modification to Design of Plant Under Construction
* LC 21 - Commissioning
* LC 22 - Modification or Experiment on Existing Plant
* LC 25 - Operational Records
* LC 35 - Decommissioning

**Note** – Detailed descriptions of each of the LC’s can be found in ONR’s Licence Condition Handbook [2].

## Health and Safety at Work etc Act 1974

1. The general duties under the Health and Safety at Work etc Act 1974 (HSWA) impose the following statutory requirements:

* 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.

## Other Relevant Legislation

1. The Construction (Design and Management) Regulations 2015 place duties on designers to recognise health and safety in the design process.
2. The Ionising Radiations Regulations 2017 reference engineering controls and design features as the primary means of restricting exposure to ionising radiation.
3. Other regulations, under the HSWA 1974, also impose duties on designers for specified engineering features.
4. Environmental Legislation, Security Legislation and International Treaties also impose legal duties on designers.

# Advice to Assessors

## Introduction

1. This TAG looks at ONR’s assessment of arrangements to design engineering equipment[[2]](#footnote-3) for use on nuclear facilities.
2. The design arrangements should:

* show that safety is integral to the design process;
* show that the safety case fully coordinates with the design activity that evolves in parallel;
* show the engineering equipment can fulfil their safety function requirements; and
* establish that the risks, as created by such arrangements, are reduced As Low As is reasonably Practicable (ALARP), and are in compliance with legal requirements.
* interface with arrangements for procurement, construction, installation and operations.
* interface with examination, maintenance, inspection and testing of engineering equipment;

1. When assessing the adequacy of design arrangements and processes ONR specialist should reference the ONRs SAPs [1] and TAGs [3]. References to the ONR SAPs, ONR’s licence conditions [2], the WENRA Reactor Safety Reference Levels [4] and IAEA Safety of Nuclear Power Plants: Design Specific Safety Requirements [5] are included in the text of this TAG.
2. Design organisations may not themselves be licensees. However, they should be under the control of the appropriate licensee. Hence, these design organisations may act as Responsible Designers to the licensee Design Authority, who themselves acts as an Intelligent Customer. ONR’s TAG on Licensee Design Authority Capability [6] relates to this and considers:

* the identification and implementation of organisational arrangements and core competencies to understand and manage the design of its plant and the safety functions that need to be provided;
* the use of contractors as ‘Responsible Designers’ to provide authoritative advice to the Design Authority; and
* the retention of design knowledge in a form that is practically and easily available to the licensee over the full lifetime of the plant until the plant is decommissioned.

1. ONR’s TAG on Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services [7] also informs ONR’s assessment of the supply chain arrangements. These arrangements are important to the supply of items or services that are significant for use in the UK. The TAG also provides guidance on ONR’s inspection during the manufacturing stages.
2. The early optioneering stages of the design process are important. Inspectors needs to strike a clear balance between the benefits of leverage (achieved by early guidance/intervention), and the potential negative disruptive effects (that occur due to detailed questioning of early concepts). Also, care should be taken not to give the impression that a design has been given regulatory approval.

## Engineering background

1. ONR SAPs ECS.1 (Safety categorisation) and ECS.2 (Safety classification of structures, systems and components) relate to the safety categorisation and classification of engineering equipment. The grading applied to the engineering equipment impacts the:

* design methods and standards;
* material selection;
* procurement process;
* fabrication;
* installation inspections;
* maintenance requirements; and
* in service inspections.

1. In any engineering process, the design resource available (whether it be in time or budget) may be limited. Hence, resources should target those hazards with the greatest potential for danger. This is the basis for all engineering safety categorisation/classification schemes.

## Design requirements and regulation

1. Design requirements normally arise because the licensee:

* Wishes to design, construct, install and commission a facility on a new site, or within an existing site. LCs 19, 20 and 21 [2] apply, as well as the requirements for site licensing for new sites.
* Wishes to undertake a modification to an existing facility. LC 22 applies [2].
* Is conducting an assessment of structures, systems and components for a periodic safety review. LC 15 applies [2].
* Wishes to decommission a facility. LC 35 applies [2].

## Design process

1. The design process is often a complex task that involves parties from different disciplines who all make a contribution to the overall design product. This design process will vary between disciplines. Issues of key importance are described in the sub-sections 4.4.1 to 4.4.23.

### Design phases

1. A good design process is the starting point for a successful design output. The design process should be clearly aligned with the safety case production process. The safety case authors, and the designers should regularly interact. All parties should recognise the need for risks associated with design solutions to be ALARP. There should be clear evidence of optioneering to support the ALARP judgement. The operators, and maintenance bodies, should be involved as early as possible. The safety important elements of the design should be recognised to enable the rigour of the safety review to be determined.
2. The design process is usually iterative, and the key requirement is that the overall risk are reduced ALARP. Any attempt to justify discrete parts of the overall design solution against the ALARP criteria may not be helpful. The safety case authors should recognise the developing design solutions. This ensures that the claims made in the safety case remain valid and accurate. A typical design process and integrated safety justification normally comprises of:

* inception and initial brief;
* feasibility studies and optioneering;
* conceptual design → preliminary safety report;
* scheme design → design freeze; and
* detailed design → design freeze → pre construction safety report.

1. Key research and development outputs should be available early in the design process. This allows the design to evolve in a logical progression.
2. The concept of design freeze is an important point in the design process. However, it should not impose absolute constraints on changes beyond this point. Any such changes to frozen information should be formally justified and the implications assessed. This is important from a safety perspective and should be thoroughly integrated into the modified design if the change is adopted. Any assessment of changes should be proportionate to the safety significance of the change.
3. It is important to recognise that when the Pre-Construction Safety Report is produced, the detailed design is normally ‘frozen’. This makes design changes difficult from a time and cost perspective. This reinforces the need for early regulatory interest in the design process. It is essential that ONR is informed of significant design changes after the issue of a licence instrument, as part of the regulatory process.
4. The design process also integrates into the project management and sanctioning processes. Several project ‘gates’ may require negotiation for the project to proceed. This sanctioning may require specific design and safety case deliverables. Continuity of design resource may be an issue as a result of this process.
5. To be highly reliable, the design process should include features such as diversity and redundancy.

### Hazard identification

1. The early identification of hazards is an important part of design safety assurance. It can use many different techniques (both inductive and deductive) that are undertaken at appropriate project design stages.   
   One such technique is ‘structured brainstorming’. This technique identifies hazards and then quantifies the worst-case credible consequence and its associated likelihood; this is usually expressed as a frequency for cumulative risk. The consequential risks, after the safeguards have been applied, are then assessed. Then, the risks are determined to be either intolerable, within the ALARP region, or in the broadly acceptable region. Any safeguards, developed as part of the hazard identification process, should be recorded and tracked through to conclusion; this ensures adequate implementation.   
   A hazard schedule, which should be treated as a live document.
2. When it is reasonably practicable to do so, fundamentally hazards should be eliminated and reduced by design. The most benefit is usually achieved at the early concept design stage.
3. On their own, document-based hazard identification studies offer limited benefit. This is because the studies may not fully recognise the complex interactions between engineering equipment. Hence, the studies should be ideally supported by other methods of hazard identification. These methods may include virtual and actual plant walkdowns during construction, installation and commissioning.
4. The hazard identification process should identify all credible postulated initiating events.
5. As the design assurance process develops, further risk assessments should be undertaken. Its format should enable the safety integrity of the design solutions to be kept.
6. ONR’s SAPs FA series (Fault analysis) [1], WENRA reference level E (Design Basis Envelope for Existing Reactors) [4], IAEA SSR 2/1 requirement 4 (Fundamental safety functions) and requirement 10 (Safety assessment) [5] apply to hazard identification.

### Optioneering

1. To demonstrate that solutions are ALARP, optioneering should be undertaken early in the design process. Optioneering is a common project management technique. Yet it often focuses on issues of cost, functionality and programme without focusing on safety. The legal requirement to reduce risks so far as is reasonably practicable (SFAIRP). This requires options relating to safety to be addressed as part of the overall design solution. Optioneering should be controlled as part of design management during the later detailed design phases. This enables the optioneering to be focused and moved forward, without each step being excessively challenged in detail. Also, microscopic level optioneering can be harmful. This is because it may not yield the best macroscopical solution, with a practical economy of effort.
2. ONR’s SAPs NT series (Numerical targets and legal limits) [1], IAEA SSR 2/1 requirement 4 (Fundamental safety functions) and requirement 6 (Safety of the plant design throughout the lifetime of the plant) [5] apply to Optioneering.

### Safety functional requirements and design parameters

1. Safety functional requirements are a set of deterministic rules that are produced at the start of the design. These rules identify the safety requirements of the engineering equipment, that are important to safety. These requirements can cascade from high level safety requirements to a larger number of lower-level functional demands on engineering equipment. The design should satisfy these requirements and update them as necessary as part of the process. These requirements should be confirmed during commissioning. They should then be fed into the operating rules and instructions, as described by LCs 23 and 24 [2].
2. The design duty (design parameters) of the engineering equipment should be identified. Examples include:

* operating temperatures;
* load combinations;
* damage and aging mechanisms;
* environmental; and
* design life.

1. These design parameters link to equipment qualification.
2. The SAPs ECS series (Safety classification and standards) [1], WENRA reference level G (Safety Classification of Structures, Systems and Components) [4], and IAEA SSR 2/1 requirement 4 (Fundamental safety functions) and requirement 6 (Safety of the plant design throughout the lifetime of the plant) [5] apply to safety functional requirements and design parameters.

### Design Planning and Organisation

1. A structured and resourced delivery plan/programme is a key part of any design process. This plan allows safety to include into the design output.   
   It achieves this by identifying the safety process requirements, such as HAZOPS and safety case integration for example. It also assists a well organised, coordinated process, without which safety cannot be demonstrated and indeed may not be achieved. The plan should identify:

* the key inputs;
* formal design outputs;
* interdependencies;
* timescales; and
* resource requirements, generally in terms of design effort including:
  + internal design skills;
  + internal facilities;
  + external skills and facilities (if external consultants are used); and
  + overall design organisation.

1. An adequate plan is a prerequisite for an effective design safety assurance process. This should be evidenced through an organisation chart.
2. Design activities may be organised as follows:

* As dedicated project teams, with personnel mixed from different technical disciplines; or
* As small project management/engineering groupings who draw effort from functional teams; organised on a discipline basis.

1. Organisations may operate with a mixture of both features.   
   Functional features can bring significant safety assurance benefits. This is because they provide shared functional knowledge, a robust verification process, collective competency and standardisation. Yet this can be a disadvantage since it discourages good communication within the project, this can lead to a ‘silo’ mentality.
2. The plan should link with the overall project, safety case, procurement and construction/installation programmes. This ensures that an effective overall project is achieved. Suitable checks should be in place to review and question the input information. This input information should not be blindly included into the design when it might be erroneous. Using this approach contributes to the defence in depth, which is an inherent feature of a highly reliable process.
3. The responsibility for the Design Authority sits at the highest level of an organisation who should always remain accountable for the design.
4. The licensee Design Authority should participate in all interactions between Responsible Designers and the ONR. This ensures that the licensee develops and maintains this Design Authority capability.
5. An effective design facility is required to adequately support the design process. Important factors for the facility include:

* the suitability of personnel and equipment; and
* the ability to access to technical and historical information.

1. Important factors for design resources are their number, continuity, turnover, training and moral. Their training of this resource should look at the following:

* consider new issues;
* include refresher training to maintain the ‘conscious competence’ mode of operation; and
* cover physical appreciation of the design of the engineering equipment, and its application within the intended facility.

1. ONR’s SAPs MS series (Leadership and management for safety) [1], WENRA reference level B (Operating Organisation) [4], and IAEA SSR 2/1 requirement 1 (Responsibilities in the Management of Safety in plant design) and requirement 2 (Management system for plant design) [5] apply to design planning and organisation.

### Design Standards

1. Technical standards should exist that underpin the design process.   
   These standards should reflect the safety classification that is assigned to the engineering equipment.
2. A range of such standards exists for nuclear design application.   
   These standards include IAEA standards, international standards, European and British standards as well as in house developed standards. Some in house standards are accepted for use with the UK nuclear industry.   
   The design organisations should have an up-to-date knowledge of the range of available standards. A mature selection process for the specific design application should be shown. The standards that are to be used should be communicated through the design organisation. Relevant training should be identified and implemented as necessary. Changes to standards must also be effectively assessed, communicated and implemented; recognising that a design standard freeze may also be put in place.
3. The SAPs ECS series (Safety classification and standards) [1] WENRA reference level C (Leadership and Management for Safety) [4] and IAEA SSR 2/1 requirement 9 (Proven engineering practices) [5] apply to design standards.

### Design verification and validation

1. Design verification is the process to confirm that each stage of the design is confirmed as correct against the requirements from the previous stage.   
   This normally entails a process of checking and approval. The following standard checking methods are usually applied:

* a direct check of the calculation; or
* design method that follows the original philosophy; or
* a check by a parallel method or calculation.

1. Normally the parallel method provides for a higher level of assurance. This is because it prevents a only arithmetical checks being undertaken; for example, on what may be an erroneous philosophy. However, a parallel check does not check intermediate results in detail. Hence, caution must be applied if these values are subsequently used. A complementary method of verification is to compare with the existing proven design. However, 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. These checks can range from checks within the originating design teams; to independent checks undertaken by external organisations.
2. Verification is normally a three-step process involving an originator, a checker and an approver. The approver should confirm there are no obvious errors; this ensures that the design output is consistent with other design elements. The approver also confirms 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. This is because they may dilute the level of individual responsibility and ownership. Aside, a culture of self-verification, i.e. ‘checking your own work’, is evident in the most effective design organisations.
3. Design validation ensures that the overall intent of the design is achieved.   
   It also prevents failure of the design intent by incremental deviation or dilution. This is achieved by combining:

* independent technical assessment;
* peer review;
* design review;
* staged testing and commissioning; and
* operating trials.

1. Where software applications are used in the design process, rigorous software validation requirements must be in force. These should include well-structured version control. Design packages may be bought in externally or developed internally. Whilst a range of software platforms can be used, 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. This software may not have been formally validated or controlled. Software should only be used for analyses when justified and validated for the specific application. The results of the analyses should be subjected to sanity checks by simplified calculations as necessary.

### The interface with procurement

1. The interface with procurement is key to ensuring that the engineering equipment that is delivered matches its design intent. Robust systems are required to firstly identifying products and materials. Inspection systems are then required to ensure that the material specified is correctly delivered by the supplier (refer to [7]). These inspection systems should verify the engineering functionality and can include type tests, batch sample tests and routine tests (including proof tests). Tests can be undertaken at the factory (Factory Acceptance 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. Such tests should be well designed to mimic as closely as practicable the duties imposed on the engineering equipment on which the design has been based and meet specified standards as necessary. The terminology surrounding testing can often be confusing. To manage this both the specifications and arrangements for testing should be technically reviewed to check they are suitable. This review is in addition to the quality assurance requirements.
2. Process should be in place to ensure that non-conformances (for equipment and material) are:

* assessed, sentenced and implemented by technically competent staff;
* categorised in terms of its safety significance; and
* if aggregate are captured, both as evidence of potential systemic process problems as well as identifying the cumulative effect on safety.

1. The SAPs EQU series (Equipment qualification) [1], WENRA reference level B (Operating organisation) [4] and IAEA SSR 2/1 requirement 23 (Reliability of items important to safety) [5] apply to the interface with procurement.

### The interfaces between design disciplines

1. The interfaces between design disciplines are important to safety. This is significant where a design covers multidisciplinary areas. Some form of interdisciplinary check should be part of any design process. Also, to ensure key issues are not missed, as well as the processes to control detailed interfaces, suitably competent engineers should understand the whole system design.

### Information control and document management

1. Information control, configuration control and document management are key requirements. This is important where large numbers of design documents are produced as part of the process. LC 17 [2] requires adequate arrangements to be made in respect of Quality Assurance (QA). LC 6 [2] also requires adequate records to be made in respect of compliance to any licence condition. Documentation, in hard copy or electronic format, is the essential output of any design process. Hence, significant effort is required to ensure that such information is clear, complete and explicit. The following safety issues are relevant:

* 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; and
* production of ‘as fitted/as built’ records.

1. WENRA reference level C (Leadership and Management for Safety) [4] and IAEA SSR 2/1 requirement 2 (Management system for plant design) [5] apply to the issue of information control and document management.

### Change control

1. The management of change is a key part of the design process. It applies 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.   
   The design information should be structured or configured in a way as to allow the agreed changes to be implemented through the design system. The general principles of design change control and associated configuration management are as follows:

* recognise the change;
* understand the safety impact of the change;
* agree the change at the correct authority level;
* control the implementation and communication of the change; and
* update of necessary documentation.

1. As the design matures, the agreement and authorisation of change is normally carried out by senior management. When the procurement and construction cycles start, the impact of the potential design changes and their implementation increase. However, resisting change because they are seen to be difficult will negatively affect safety. This is because the required changes will not be recognised and sentence as appropriate.
2. If incorrect management of changes is applied, this can result in inadequately conceived and/or executed changes. Hence, the potential impact on safety can be substantial.

### Competency

1. LC 12 [2] requires that only Suitably Qualified and Experienced Persons, (SQEPs), should perform any duties that may affect safety. As this requirement also affects designers, the competence of the design resource should be reviewed internally. This review should recognise the skills, technical discipline and experience of the designers and design management. It should only be undertaken by suitably qualified and experienced personnel.
2. WENRA reference level B (Operating Organisation) [4] and IAEA SSR 2/1 requirement 3 (Safety of the plant design throughout the lifetime of the plant) [5] apply to the issue of competency.

### The interface with construction/installation

1. The design process should clearly link to the construction/installation process. This should allow adequate information to be provided to the construction teams. A process should be in place 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. LCs 19 and 20 [2] are relevant to this issue.   
   Arrangements should be in place to ensure that non-conformances are recognised, assessed at the correct level and suitably sentenced by a controlled process.

### The interface with commissioning

1. The design process should link to the commissioning process. This should allow adequate information to be provided to the commissioning teams.   
   A process should be in place 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.   
   LC 21 [2] has 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.
2. The commissioning process should confirm the assumptions made and requirements identified through the design process.
3. The SAPs ECM series (Commissioning) [1] and IAEA SSR 2/1 requirement 4 (Fundamental safety functions) [5] apply to the interface with commissioning.

### The Interface with Maintenance and Inspection

1. The design process should identify the examination, inspection, maintenance and testing requirements of the engineering equipment.   
   This supports continued safe operation. The design process should consider:

* the visibility and accessibility of items of engineering equipment; and
* items that need replacing within the design life of the facility.

1. LC 28 [2] is relevance to this issue.
2. The SAPs EMT series (Maintenance, inspection and testing) [1], WENRA reference level K (Maintenance, In-service inspection and Functional Testing) [4] and IAEA SSR 2/1 requirement 6 (Design for a nuclear power plant) [5] are applicable to the interface with maintenance and inspection.

### Safety case production and interface

1. The design process must lead to the production of safety documentation that achieves the required level of assurance. Reference should be made to the relevant BMS guidance.
2. It is normal for the safety case format to follow a logical (claim, evidence, argument) type chain. The design process should also enable evidence of the design information and parameters to be provided.
3. Existing facilities are often subject to upgrade programmes. Hence, the existing state of the facility and its original design intent are important inputs into the design and safety case production activities. If this information is unavailable, it can be got from the engineering substantiation process.
4. The SAPs SC series (Safety cases) [1] and WENRA reference level N (Contents and updating of Safety Analysis Report) [4] are applicable to safety case production and interface.

### Design review

1. The quality management system should identify the need to carry out design reviews. Timely reviews should confirm the validity of the design.   
   These reviews can act as a forum for information transfer, identify problem areas, and give direction to solutions. These reviews should be supported, and their importance recognised. Procurement, construction and installation persons should participate if practicable. Normally, a design review should:

* identify and meet the requirements of the brief;
* establish and meet appropriate design acceptance criteria;
* integrate the safety justification and design process;
* establish the correct design parameters;
* identify the materials and products;
* produce suitable, and referenced, design documentation; and
* identify suitable limits and conditions of safe operation.

### Design instructions

1. A process should be in place that ensures that design instructions are available. These instructions should be formally generated, suitably verified, controlled and distributed.

### Fault Recording and Corrective Action Systems

1. A process should be in place to ensure that that design related faults and related improvements are fed back to the designers. These are normally identified from a range of different sources. i.e. procurement, construction, installation, commissioning, final operation and maintenance etc.   
   This process is sometimes termed a ‘fault recording and corrective action system’ that normally follow the following model:

* record and understand the fault;
* identify what project action is required for existing designs/materials/installations;
* identify what project action is required for future designs/materials/installations; and
* identify what changes to design processes may be required in the future.

1. Normally ‘lessons learned’ workshops can provide a valuable learning. They can be used to ensure that difficulties are minimised for the future. These workshops should also identify positive features, as well as areas for improvement. This ensures that good practice is repeated in the future.
2. WENRA reference level J (System for Investigation of Events and Operational Experience Feedback) [4] and IAEA SSR 2/1 requirement 2 (Management system for plant design) [5] apply to fault recording and corrective action systems.

### Intelligent Customer and Design Authority

1. The design knowledge should be kept in a form that can be retrieved and is easily understood. This applies to the lifetime of the facility’s operational and decommissioning periods. The licensee Design Authority is responsible for:

* maintaining the necessary engineering skills and knowledge;
* implementing appropriate research; and
* dealing with intellectual property issues as required.

1. In situations where the design is contracted out, it is important that the licensee retains the Design Authority and Intelligent Customer roles. Keeping these roles allow the licensee to:

* specify the design requirements;
* monitor the design delivery process and validate the output;
* retaining corporate knowledge;
* review the third party design consultants, i.e. the Responsible Designer; and
* interface with procurement and construction/installation.

1. Reference should be made to [6], which addresses ONR’s expectations for existing and prospective licensees’ Design Authority capability.
2. WENRA reference level C (Leadership and Management for Safety) [4] and IAEA SSR 2/1 requirement 2 (Management system for plant design) [5] apply to the issue of intelligent customer and design authority.

### Human factors

1. Human factors is important throughout the design process. The design of engineering equipment should sufficiently recognise human factors. This is in terms of application of design standards, installation, subsequent operation maintenance and decommissioning. Designers may unintentionally create assemblies which only ‘work’ in their final configuration. They may not consider how they can be safely assembled or maintained. Also, given designers often focus on ensuring that configurations do successfully work, they may fail to question how they could be misused or fail. This relates to the systematic assessment of what could go wrong at a detailed level.
2. Human factors assessment should input into the design process. This is to ensure that demands on operators to operate the equipment, maintain it and recovery from failures are adequately assessed. When considering the final configuration physical mock-ups, as well as theoretical and computer-based models, can play an important part in linking the design concepts to human factors issues.
3. Where necessary, guidance should be sought from specialist human factors practitioners.
4. The SAPs EHF series (Human factors) [1] and IAEA SSR 2/1 requirement 6 (Design for a nuclear power plant) [5] apply to the issue of human factors.

### Design quality assurance

1. Design activities should be internally regulated against suitable set of quality assurance procedures. This activity should be subject to internal audit with evidence of observations, corrective actions and close out.
2. WENRA reference level C (Leadership and Management for Safety) [4] and IAEA SSR 2/1 requirement 2 (Management system for plant design) [5] apply to design quality assurance.

### Design for decommissioning

1. The design should identify the need to decommission facilities and its equipment. As well as decommissioning the facility, engineering equipment may need to be replaced as its design life expires. Features that support operational safety may be difficult to substantiate for decommissioning.   
   For example, an engineering components seismic capability may require substantial structural engineering solutions to support decommissioning. Recognising the future requirements at the design stage should allow the best solution to be achieved; whilst still ensuring safety at all stages. LC 35 [2] is relevance to this issue.
2. The SAPs DC series (Decommissioning) [1] and IAEA SSR 2/1 requirement 3 (Safety of the plant design throughout the lifetime of the plant) [5] apply to the issue of design for decommissioning.

# Summary

1. This TAG advises the reader of key elements of the design process that are associated with items important to safety. It focuses on application within the nuclear environment.
2. The detailed features of the design process itself will vary between disciplines and projects. However, this document covers the key elements which should exist within an effective design organisation that produces design solutions that will be demonstrably safe. These elements can be sampled, assessed and inspected as required. They form part of the regulatory process to gain assurance of nuclear, security and transport safety.

# Bibliography and Further Reading

The Tolerability of Risk from Nuclear Power Stations, Revised 1992. Reducing risk, protecting people, HSE’s decision-making process, 2001.

Quality management systems – Requirements, BS EN ISO 9001:2015.

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.

BS 7000 Design management systems

BS 7000-1:2008 Guide to managing innovation

BS 7000-2: 2015 Guide to managing the design of manufactured products

BS 7000-4: 2013 Guide to managing design in construction

BS 7000-10: 2008 Vocabulary of terms used in design management

DOE Standard Configuration Management, US Department of Energy (DOE-STD-1073-2016).

Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, IAEA, 2003.

Licensing Nuclear Installations, November 2021.The Office for Nuclear Regulation.

# References

|  |  |
| --- | --- |
| [1] | ONR, “Safety Assessment Principles (SAPs) for Nuclear Facilities - 2014 Edition (Revision 1),” January 2020. [Online]. Available: https://www.onr.org.uk/saps/saps2014.pdf. |
| [2] | ONR, “ONR Licence Condition Handbook,” Febuary 2017. [Online]. Available: https://www.onr.org.uk/documents/licence-condition-handbook.pdf. |
| [3] | ONR, “ONR Technical Assessment Guides,” [Online]. Available: https://www.onr.org.uk/operational/tech\_asst\_guides/index.htm. |
| [4] | WENRA, “Safety Reference Levels for Existing Reactors 2020,” 2021. |
| [5] | IAEA, “IAEA Safety Standards - SSR-2/1 - Safety of Nuclear Power Plants: Design”. |
| [6] | ONR, “NS-TAST-GD-079 - Licensee Design Authority Capability”. |
| [7] | ONR, “NS-TAST-GD-077 - Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services”. |

# Glossary and Abbreviations

ALARP As Low As Reasonably Practicable

FAT Factory Acceptance Test

IAEA International Atomic Energy Agency

QA Quality Assurance

SAT Site Acceptance Test

SAP Safety Assessment Principle(s)

SQEPs Suitably Qualified and Experienced Persons

TAG Technical Assessment Guide(s)

WENRA Western European Nuclear Regulators’ Association

1. ALARP (As Low as is Reasonably Practicable) and SFAIRP (So Far As is Reasonably Practicable) are used interchangeably. [↑](#footnote-ref-2)
2. Engineering equipment is the term given for engineering structures, systems and components. [↑](#footnote-ref-3)