Office for Nuclear Regulation

ONR GUIDE			
Licensee Design Authority Capability			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-079 Revision 3		
Date Issued:	April 2016	**Review Date:**	April 2019
Approved by:	David Senior	Programme Director	
Record Reference:	TRIM Folder 1.1.3.776. (2016/168640)		
Revision commentary:	Fit for purpose review		

TABLE OF CONTENTS

Published 04/16

1. INTRODUCTION

1.1 ONR has established its Safety Assessment Principles (SAPs) MS.1 to MS.4 which apply to the assessment by ONR specialist inspectors of the organisational capability of potential and existing licensees. The principles presented in these SAPs are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide is one of those guides.

2. PURPOSE AND SCOPE

2.1 This TAG sets out ONR's expectations for existing and prospective licensees' Design Authority capability. It considers the licensee's approach to:

- Identification and implementation of organisational arrangements and the core capability 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;
- 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.

2.2 The following definitions are applicable to this assessment guide:

- **Design** – the result of developing a concept, detailed plans, supporting calculations and specifications for a facility and its parts.
- **Design Process** – the conversion of inputs such as basic functional and performance requirements, safety goals and safety principles, applicable codes, standards and regulatory requirements into a design.
- **Design Authority** – the defined function of a licensee's organisation with the responsibility for, and the requisite knowledge to maintain the design integrity and the overall basis for safety of its nuclear facilities throughout the full lifecycle of those facilities. Design Authority relates to the attributes of an organisation rather than the capabilities of individual post holders.
- **Responsible Designer(s)** – organisations which have a formal responsibility for maintaining detailed, specialised knowledge of all the systems and components important to safety, and a core capability in the detailed design process.
- **Design Authority Intelligent Customer –** 'Intelligent Customer' is defined and described in T/AST/049 'Licensee use of contractors and intelligent customer capability'. Where a licensee relies upon a Responsible Designer(s), the Design Authority should act as an Intelligent Customer by specifying requirements, supervising the work and technically reviewing the output before, during and after implementation. The Design Authority Intelligent Customer role is highlighted separately from the normal intelligent customer role in this TAG because of the specialist knowledge of plant design and the nuclear safety case required to fulfil it.
- **Core Capability** – the knowledge, functional specialisms and resources that the licensee should maintain within its own organisation to be able to maintain control and oversight of safety at all times.

2.3 A licensee may use different terminology to the particular words chosen above. The Inspector should satisfy himself that the required functions are fulfilled, preferably identifying direct parallels for the bodies identified above.

2.4 It is recognised that different arrangements apply for defence sites in respect of Design Authority arrangements for submarine reactors and nuclear warheads. In these cases the Design Authority will be separate from the licensee and the licensee's responsibility will be to co-operate intelligently with the Design Authority to ensure that the activities conducted by the licensee relating to submarine reactors or nuclear warheads are safe. Many of the attributes of a licensee described in this TAG will still be relevant. The Defence Nuclear Safety Regulator is specifically required to regulate the design of, and Design Authority arrangements for, submarine reactors and nuclear warheads. It works closely with ONR in respect of safety at defence licensed sites.

3. RELATIONSHIP TO NUCLEAR SITE LICENCE AND OTHER LEGISLATION

The following UK legal and other requirements are applicable to the establishment and maintenance of an effective Design Authority:

3.1 Health and Safety at Work etc Act (1974)

- Section 2 requires every employer to provide and maintain plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health;
- Section 6 places duties on any person who designs, manufactures, imports or supplies any article for use at work[1] thus:
- To ensure, so far as is reasonably practicable, that the article is so designed that it can be constructed, operated and decommissioned in a manner that will be safe and without risks to health at all times;
- To carry out or arrange for the carrying out of such testing and examination as may be necessary for the performance of the duty imposed by the preceding paragraph;
- To take such steps as are necessary to ensure that the persons supplied with the article are provided with adequate information about the use for which the article is designed or has been tested and about any conditions necessary to ensure that, so far as is reasonably practicable, it will be safe and without risks to health at all times.
- To take such steps as are necessary to ensure that the persons supplied with the article are informed of any discovery that an aspect of the design gives rise to a serious risk to health or safety.
- To carry out or arrange for the carrying out of any necessary research with a view to the discovery and, so far as is reasonably practicable, the elimination or minimisation of any risks to health or safety to which the design or article may give rise.

3.2 Management of Health and Safety at Work Regulations (1999)

- Regulation 5 requires employers to have arrangements as appropriate for the effective planning, organisation, control, monitoring and review of the preventative and protective measures;

[1] For defence licensed sites, in respect of submarine reactors and nuclear warheads, these duties are the responsibility of the design authority separate from the licensee (see paragraph 2.4).

- Regulation 7 requires an employer to appoint competent persons to assist him in undertaking the measures he needs to comply with the requirements and prohibitions imposed on him.

3.3 Construction (Design and Management) Regulations (2015)

- These regulations impose requirements with respect to the design and management aspects of construction work. A licensee should be able to demonstrate the ability to understand, monitor and direct the nuclear safety aspects of construction work.

3.4 Nuclear Installations Act (1965) as amended (NIA)

- The NIA requires HSE to attach conditions to nuclear site licences as necessary in the interests of safety.

3.5 Nuclear Site Licence Conditions

- **LC 6 – Documents, Records, Authorities and Certificates**. The licensee shall make adequate records to demonstrate compliance with any of the conditions attached to the nuclear site licence. The Design Authority has a key functional role to provide and maintain a through life record and configuration system.
- **LC 10 – Training**. The licensee shall make and implement adequate arrangements for suitable training of all those on site who have responsibility for any operations which may affect safety. Staff fulfilling Design Authority or Responsible Designer roles, as roles which may affect safety, must be suitably trained to fulfil those roles.
- **LC 12 – Duly Authorised and Other Suitably Qualified and Experienced Persons**. The licensee shall make and implement adequate arrangements to ensure that only suitably qualified and experienced persons perform any duties which may affect the safety of operations on the site. Persons fulfilling Design Authority or Responsible Designer roles, as roles which may affect the safety of operations, must be suitably qualified and experienced to fulfil those roles.
- **LC 23 – Operating Rules**. The licensee shall, in respect of any operation that may affect safety, produce an adequate safety case[2] to demonstrate the safety of that operation and to identify the limits and conditions, referred to as operating rules, necessary in the interests of safety. For new plants, the Design Authority should establish, and be able to justify, the conditions and limits. Proposed design changes should be considered by the Design Authority in the context of the safety case and potential impact on the operating rules.
- **LC 36 – Organisational Capability.** This condition requires a licensee to provide and maintain adequate financial and human resources to ensure the safe operation of the licensed site, and to make and implement adequate arrangements to control any change to its organisational structure or resources which may affect safety.

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

Safety Assessment Principles (SAPs)

[2] LC 14 – Safety Documentation deals with the arrangements for 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.

4.1 The Safety Assessment Principles for Nuclear Facilities (2006 Edition, Revision 1) provides a framework to guide regulatory decision making in the nuclear permissioning process. It is supported by Technical Assessment Guides (TAGs) which further aid the decision-making process. The following principles are of particular relevance to this Technical Assessment Guide:

- MS.1. Leadership. Identifies the need for directors, managers and leaders to focus the organisation on achieving and sustaining high standards of safety and on delivering the characteristics of a high reliability organisation.
- MS.2. Capable Organisation. Identifies the need for an organisation to have the capability to secure and maintain the safety of its undertakings;
- MS.3. Decision Making. Identifies the need for decisions at all levels that affect safety to be rational, objective, transparent and prudent;
- MS.4. Learning From Experience. Identifies the need for lessons learned from internal and external sources to continually improve leadership, organisational capability, safety decision making and safety performance.

Technical Assessment Guides (TAGs)

4.2 The following Technical Assessment Guides are applicable to this TAG:

- T/AST/048 – Organisational Capability

  This TAG sets out the broad principles which underpin ONR's expectations of a licensee's arrangements to provide and maintain adequate financial and human resources and to control changes to its organisation structure or resources which may affect safety.

- T/AST/49 – Licensee Core and Intelligent Customer Capabilities

  This TAG sets out some broad principles which underpin ONR's expectations of a licensee's arrangements for the use of contractors and for retaining control of nuclear safety.

- T/AST/057 – Design Safety Assurance

  This TAG addresses the means by which the licensee demonstrates how safety is integrated into the design production process and, in particular, the responsibility of the Design Authority for the functionality of the completed design product where design is undertaken by different organisations.

- T/AST/065 – Function and Content of the Nuclear Baseline

  This TAG addresses the means by which the licensee demonstrates that its organisational structure, staffing and competencies are, and will remain, suitable and sufficient to manage nuclear safety throughout the full range of the Licensee's business. It provides the foundation from which organisational changes can be assessed.

- T/AST/072 – Function and Content of a Safety Management Prospectus

  Element 7 of this TAG expects a licensee to understand its processes and plant, and to ensure that knowledge is captured and managed.

Licensing of Nuclear Installations (ONR 2012)

4.3 Paragraphs 81, 82 and 83 set out ONR's expectations of a licensee's intelligent customer and design authority capabilities, including the requirement for the licensee to have sufficient, suitably qualified and experienced staff, and for the creation of a

Design Authority function within the licensee. Paragraph 83 also expects the licensee to develop a process for the transfer of knowledge from the designer to the licensee.

WENRA Reactor Safety Reference Levels

4.4 The objective of The Western European Nuclear Regulators Association (WENRA) is to develop a common approach to nuclear safety in Europe by comparing national approaches to the application of IAEA safety standards. There is no direct reference to Design Authority in the Reactor Harmonisation Working Group Reference Levels, 2008. However, the reference levels in the following harmonisation issues represent good practices in the WENRA member states are relevant and should be taken into account by the Inspector:

- Issue B: Operating Organisation. Identifies the need for the organisational structure for safe and reliable operation of the plant to be justified and documented.
- Issue C: Management System. Identifies the need for the management system to achieve and enhance nuclear safety by ensuring that other demands on the Licensee are not considered separately from nuclear safety requirements.
- Issue Q: Plant modifications. Identifies the need for a process which ensures that all permanent and temporary modifications are properly designed, reviewed, controlled, and implemented, and that all relevant safety requirements are met.

IAEA Safety Standards

4.5 The IAEA Safety Standards (Requirements and Guides) were the benchmark for the revision of the SAPs in 2006 and are recognised by ONR as relevant good practice. They should therefore be consulted, where relevant, by the Inspector, although it should be appreciated that they are design standards rather than regulatory standards.

4.6 The IAEA Safety Standards do not address the issue of the Design Authority explicitly but the Safety Requirements publication GS-R-3 ‘The Management System for Facilities and Activities’ (IAEA 2006) is relevant. It defines the requirements for establishing, implementing, assessing and continually improving a management system.

4.7 The following report produced by the International Nuclear Safety Advisory Group (INSAG) for the IAEA is also directly relevant:

- INSAG 19 ‘Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life’. This report discusses the problem of maintaining the integrity of the design of a nuclear plant over its entire lifetime in order to achieve a continuous high level of safety.

5. ADVICE TO INSPECTORS

Background

5.1 A nuclear plant design is the product of the activities of many organisations, and changes to that design may occur periodically over the plant’s lifetime. Maintaining the level of safety expected of a nuclear facility requires that changes to it must be made with full knowledge of the design and the safety functions that need to be provided. This knowledge has to be retained in a form that is practically and easily available to the licensee over the full lifetime of the plant until the plant is decommissioned.

5.2 A licensee should have a formal process to understand and maintain design knowledge and design integrity. That part of the licensee's organisation with the responsibility for, and the requisite knowledge to maintain, the design integrity and the overall basis for safety of its nuclear facilities throughout the full lifecycle of those facilities is termed the 'Design Authority'[3].

5.3 ONR expects existing licensees to have a suitable and sufficient Design Authority capability and organisations seeking to become nuclear licensees to have credible programmes to develop this capability in a timely manner.

5.4 The Design Authority should have sufficient knowledge to understand the safety case requirements for the plant and to assess the impact of proposed design changes on the functionality, reliability and availability claims made in the safety case. The Design Authority should also have sufficient knowledge of any specific constraints that impact on the practical use of the plant and thereby need to be reflected in an effective design, such as restrictions in space, availability of site services, discharge authorisation limits, conditions for acceptance in the case of waste processing plants etc. These factors should be considered at the same time as the generic design inputs, such as legislative requirements.

5.5 Ownership of the safety case and responsibility for understanding the function and performance of existing plant should ordinarily reside with the operations function, rather than with the Design Authority. For new plant, the Design Authority may be the owner of the safety case during the design/construction phase prior to the operations function being established. The Design Authority should be expected to maintain this 'Design Safety Case' through life, which should include:

- Recording plant modifications effected to improve performance or made in the light of operating experience;
- Approving design substantiations for any modification proposed;
- Recording of operating experience which might impact the design across all plant operators, and analysis thereof to identify trends and the need for essential plant upgrades, tighter operating constraints etc. to maintain safety;
- Communication of the need for essential plant upgrades, tighter operating constraints etc. to maintain safety across all operators;
- Effecting essential research, through-life degradation testing etc. to support safety to end of design life and likely life extension to be requested by the operators.

5.6 ONR recognises that, for new plant, the vendor rather than the licensee may own the design. Where this is the case, ONR will expect the licensee to demonstrate how it proposes to acquire a suitable and sufficient Design Authority capability.

5.7 ONR also acknowledges that the licensee may not have all the detailed, specialised knowledge required of all the systems and components important to safety within its Design Authority organisation. In such instances it may assign its responsibilities for some parts of the plant to other organisations such as those that originally designed the plant. Bodies with these responsibilities are termed 'Responsible Designers'. The licensee should be able to demonstrate how it intends to maintain a satisfactory contractual relationship to deliver the Responsible Designer service from the vendor for the foreseeable future, if this cannot cover whole plant life.

[3] Although the licensee may deliver the Design Authority function via a body with a difference title, ONR expects that the Design Authority capability can be identified within the licensee organisation.

5.8 The licensee must retain sufficient knowledge of all aspects of the design to act as a 'Design Authority Intelligent Customer' to enable it to understand the results of the Responsible Designers' work, and to understand the implications of that work for the life of the plant. The licensee must also understand any implications from the design for other plant and safety related systems on its site (for example emergency arrangements).

5.9 The relationship between licensee/future licensee organisation, core capability, Design Authority, Design Authority Intelligent Customer and Responsible Designer is illustrated in Annex 1. The roles of Design Authority and Design Authority Intelligent Customer should be part of the licensee's core capability and included in the licensee's Nuclear Baseline.

5.10 The aim of this TAG is to help Inspectors consider whether licensees have identified their Design Authority needs and established suitable and sufficient capabilities and processes to meet these needs. In line with the SAPs and the Principles of Better Regulation, regulatory attention to Design Authority capability will be commensurate with the magnitude of the hazard, although issues such as novelty and uncertainty of the design will also be factors.

5.11 This TAG represents ONR's view of good practice and ONR would expect a Design Authority capability established for a new facility to satisfy the expectations which are set out in this document. For existing licensees and existing plant, ONR expects that a gap analysis will be undertaken and ALARP improvements made.

Design Authority Capability Principles

5.12 There are some broad principles which underpin the ONR's expectations of a licensee's Design Authority capability. These are summarised below and interpreted in the sections that follow:

1. The Design Authority should be a defined function within a licensee's organisation which is independent of operations and has a clearly defined reporting line to the Board of the licensee organisation;
2. The Design Authority should have the authority and the responsibility to approve or reject proposed design changes and concessions;
3. The Design Authority should have the capability to understand the totality of the design and nuclear safety case in the context of each stage of the full plant lifecycle;
4. The Design Authority should have the resources, capability and management processes to assess changes to the plant's conditions and limits and performance characteristics, and have the authority to recommend modification to or suspension of operations;
5. The Design Authority should have appropriate up to date knowledge, skills, experience and resources;
6. The Design Authority should regularly assess and determine the continued adequacy of the plant's design and safety case, and have the authority and responsibility to respond to the issues identified.
7. Where the Design Authority does not have the detailed, specialised knowledge required of all the systems and components important to safety it may choose to assign those responsibilities to 'Responsible Designers' using the supply chain.

Principle 1

The Design Authority should be a defined function within a licensee's organisation which is independent of operations and has a clearly defined reporting line to the Board of the licensee organisation.

5.13 It is expected that the Design Authority capability will be delivered by a defined function within a licensee's organisation which is independent of operations to avoid a potential conflict of interest with the operations functions.

5.14 There should be a Design Authority functional head to provide authority and credibility within the organisation. The Head of Design Authority should have a reporting line to the Board of the licensee organisation, either directly or through an Executive Board Director, to enable the Board to receive an authoritative view.

5.15 The licensee may choose to fulfil the Design Authority capability either through a single Design Authority department or by distributing it amongst several fully competent departments responsible to the Design Authority functional head. Under this arrangement, each department should be headed by an 'authorised designer' who has the requisite knowledge and experience of the design and nuclear safety case for the parts of the nuclear plant or nuclear facilities that they have Design Authority responsibility for. The Design Authority functional head should retain oversight and assurance of the totality of the Design Authority capability.

5.16 SAP SC.8 notes that ownership of the safety case should reside within the licensee's organisation with those who have direct responsibility for safety. Whilst the Design Authority should have sufficient knowledge to understand the safety case it may or may not own the safety case production process.

5.17 The organisational arrangements should be clearly defined and documented in the licensee's management system, and roles and responsibilities should be clearly understood throughout the licensee organisation.

5.18 The Inspector should consider whether or not:

- The licensee's organisation structure will deliver the requirements of a Design Authority;
- The Design Authority capability is a defined function within the licensee organisation;
- The Design Authority organisation structure been substantiated through the Nuclear Baseline process.
- The Design Authority is independent from operations and has a direct reporting line to the licensee Board;
- The Design Authority functional head and staff are SQEP for the role, and are able to demonstrate that are an intelligent customer for the information they receive about nuclear safety;
- There are clear lines of accountability and control for the Design Authority capability traceable right through the organisation;
- The relationships between the Design Authority, staff responsible for the production and maintenance of safety case, plant operators and engineering/maintenance are staff clearly understood and working in accordance with the management system;

- The Design Authority capability, Responsible Designer and Design Authority Intelligent Customer roles and responsibilities are fully documented within the Management System;
- The effectiveness of the Design Authority is measured and monitored i.e. using key performance indicators.

Principle 2

The Design Authority should have the authority and the responsibility to approve or reject proposed design changes and concessions.

5.19 For existing plant, maintaining the very high level of safety expected of a plant requires that design changes are made with a full understanding of all the design information and the potential impact on nuclear safety of proposed changes. The Design Authority should be engaged in modifications at an appropriate level and have ultimate authority to approve or reject proposed design changes. Licensees should have a process to determine the appropriate level of Design Authority involvement.

5.20 The capability and authority to reject proposed design changes that do not maintain the design integrity is an important role of the Design Authority. This role should be clearly defined and documented in the licensee's Management System.

5.21 ONR expects that the supply chain will make every effort to deliver 'right first time quality. However, from time to time deviations (non-conformances) from the purchaser's technical specification may occur at any level within the supply chain. The control of any such deviations from the technical specification is fundamental to the achievement of quality and therefore the integrity of the item.

5.22 The licensee should have arrangements in place which ensure that suppliers at all levels in the supply chain identify and categorise deviations for items or services should they arise. These should include referring any deviations from the technical specification to the Design Authority for assessment and approval in the form of a concession or procedure for re-work for. These arrangements should ensure that the impact on the safety case is assessed and be clearly documented in the licensee's Management System.

5.23 In the event that a project is managed by a Tier 1 contractor on behalf of the licensee, the licensee should ensure that responsibilities for the management of deviations are clearly defined between the parties and that the arrangements ensure that all concessions for deviations from the technical specification are assessed and sentenced by the Design Authority.

5.24 If the licensee chooses to delegate responsibility for sentencing concessions that do not have an impact on the technical specification, it should ensure that the Design Authority is notified of all such concessions and has the authority to overturn the Tier 1 contractor in the event that it considers that the concession has been incorrectly sentenced. The Design Authority should also maintain oversight of the totality of concessions on the project.

5.25 The licensee should have a formal and rigorous design change process which ensures that the actual configuration of the plant throughout its life is consistent with the design, and that changes are made with the full knowledge of the design intent.

5.26 The Inspector should consider whether or not:

- The Design Authority has got the formal authority to approve/reject proposed design changes and that this is documented in the Management System;

- The Design Authority is involved in the assessment of proposed modifications to plant on a proportionate basis;
- The modification process gives confidence that changes to plant are being made with full knowledge of the design intent.

Principle 3

The Design Authority should have the capability to understand the totality of the design and nuclear safety case in the context of each stage of the full plant lifecycle.

5.27 The long lifetime (construction, commissioning, operation and decommissioning) of nuclear plants means that a plant will undergo changes throughout its life. Changes can include physical ageing of the plant's systems, structures and components, software and hardware obsolescence, feedback from operating experience or research and development, changing engineering or regulatory standards, changes in plant performance, change of lifecycle phase and changes in the licensee organisation or operating practices.

5.28 It is essential that the Design Authority retains the capability to understand the totality of the design and nuclear safety case over the full construction, operation and decommissioning lifetime of the plant. This capability should be in the form of both knowledge i.e. information and records, and expertise. Knowledge should be available in a form that is practically and easily available to those who need access to it.

5.29 The Design Authority should have arrangements in place to engage with the licensee's Nuclear Safety Committee as and when necessary.

5.30 Knowledge of the design typically expected of a Design Authority is given in Annex 2.

5.31 The Inspector should consider whether or not:

- The Design Authority has the capability to fully understand the totality of the design and nuclear safety case at the current and future stages of the plant lifecycle;
- The Design Authority is kept systematically informed of all relevant strategies within the licensee's organisation (operational strategies, decommissioning strategy etc.);
- Where a plant is about to transition from one stage of its lifecycle to another, the Design Authority is able to demonstrate that it understands, and will have, sufficient capability to support that stage of the plant's lifecycle;
- The Design Authority has got adequate knowledge management arrangements through which it can demonstrate that it has a detailed understanding of the design knowledge required in Annex 2;
- Plant records i.e. drawings, specifications etc. are up to date and reflective of the current status of the plant;
- Knowledge is available to those who need to access it;
- There are adequate arrangements in place to manage the quality of information and access to it.

Principle 4

The Design Authority should have the resources, capability and management processes to assess changes to the plant's conditions and limits and

performance characteristics, and have the authority to recommend modification to or suspension of operations.

5.32 Design changes are not limited to plant modifications. Changes can occur to the way in which a plant is operated, and the implications of operating experience on the design may also need to be taken into account.

5.33 The plant operator should be obliged to inform the Design Authority of any changes it wishes to implement that may have a significant impact on the safety performance of the plant.

5.34 The Design Authority should have the ability to understand and justify the technical basis of plant operations. It should be able to assess the impact of operational and performance related changes and to provide advice and guidance to the operations function. This should also include formal authority to recommend modification to or suspension of operations if it considers that the plant is being, or may be, operated in a manner which compromises safety.

5.35 This role should be clearly defined and documented in the management system.

5.36 The Inspector should consider whether or not:

- Arrangements exist to ensure that the Design Authority's knowledge of a plant's operating regime and performance characteristics remains current;
- Knowledge is available to those who need to access it in the licensee organisation;
- The performance of a plant is evaluated and there is a process to compare it with the safety case;
- There is a process for the Design Authority to raise concerns about the way a plant is being operated which includes a description of how potential differences of opinion with the plant operator will be resolved;
- The Design Authority's authority to recommend modification to or suspension of operations is formally recorded in the management system, and that this authority is clearly understood by operations function;
- There is evidence to demonstrate that changes to a plant operating regime have been assessed by the Design Authority and the appropriate decision has been justified and formally recorded in the knowledge management system.

Principle 5

The Design Authority should have up to date knowledge, skills, experience and resources.

5.37 Failure to ensure full knowledge of how plant design is maintained and to manage design changes may, over the lifetime of the plant, result in decisions being taken about proposed design changes or modifications without a full understanding of the effect that these decisions may have on the safety of the plant.

5.38 The Design Authority should ensure that a knowledge base of SQEP staff is established, preserved and expanded with experience. The knowledge of the design which is needed for the safe operation and maintenance of a plant should be available to all parts of the licensee.

5.39 The Design Authority should ensure that the necessary engineering and scientific knowledge, skills and experience are maintained as part of the nuclear baseline, and that sufficient resources are available to fulfil its role.

5.40 Resource management should be integrated with formal human resource processes. Succession plans should be in place for specialist and singleton resources and contingency plans available to cover the unexpected loss of key resources.

The Inspector should consider whether or not:

- The knowledge base of SQEP staff is being adequately maintained;
- Arrangements are in place to ensure that the informal knowledge held by key individuals is captured in the knowledge management system;
- There a comprehensive resource strategy with evidence of proactive management including succession planning for the Design Authority capability;
- The Design Authority capability is clearly identified as a core capability with safeguards in place to prevent it being degraded through inadequately controlled changes, leading to over-reliance on contractors;
- There is evidence that the Design Authority capability is kept under review in order to maintain a licensable organisation.

Principle 6

The Design Authority should regularly assess and determine the continued adequacy of the plant's design and safety case, and have the authority and responsibility to respond to the issues identified.

5.41 The Design Authority should have a proactive approach which enables it to regularly assess the adequacy of the plant's design and safety case as an integral part of a licensee's assurance process. This should include full and immediate access to relevant information from all parts of the licensee organisation and Responsible Designers.

5.42 Reviews should be carried out covering topics such as plant performance, effectiveness of modifications, structural integrity, plant reliability, maintenance periodicity, system and component common cause failures and failure modes. The output of the reviews should be disseminated throughout the licensee organisation, used to continuously improve the safety of the plant, and to inform Periodic Safety Reviews.

5.43 The Design Authority should maintain (or ensure that Responsible Designers maintain) up to date records of all the drawings, specifications, manuals, design standards, engineering calculations, supporting data and theoretical bases for the plant systems, structures and components.

5.44 The Design Authority should have arrangements in place to ensure that it learns from operating experience inside and outside the licensee organisation and have the capability to understand the implications for the plant design. The learning should be incorporated into the knowledge base and disseminated throughout the licensee organisation.

The Inspector should consider whether or not:

- The Design Authority has systems in place to ensure it acts from a basis of the best available information, from both within and outside its own organisation;

- There is a process in place to enable the Design Authority to continually asses the adequacy of the plant's design and safety case;
- The process is effective in identifying areas for improvement in safety performance and learning opportunities;
- Plant records i.e. drawings, specifications etc. are up to date and reflective of the current status of the plant;
- There is evidence to demonstrate that the Design Authority has a learning and improvement process that includes receiving and acting on learning and experience from inside and outside the nuclear industry.

Principle 7

Where the licensee does not have all the detailed, specialised knowledge required of all the systems and components important to safety, it may choose to assign those responsibilities to 'Responsible Designers' using the supply chain.

5.45 Although a Design Authority may assign some responsibilities to Responsible Designers, it cannot delegate its overall responsibility for the integrity of the totality of the design. It should retain sufficient knowledge of all aspects of the design to enable it to understand the results of the Responsible Designers' work, and to understand the implications of that work for the rest of the design through its role as an 'Intelligent Customer'.

5.46 The relationship between the Design Authority, as a part of the licensee's organisation, and Responsible Designers should be formalised under contract. The licensee should clearly demonstrate the attributes of an Intelligent Customer under these arrangements.

5.47 Responsible Designers should have a formal contractual responsibility for maintaining their specialised knowledge of design and their competence in the detailed design process. The contractual arrangements should include provision for the Design Authority and, if requested, the ONR to assess the level of knowledge and competence via inspection.

5.48 The contractual arrangements should ensure adequate security of, and accessibility to, knowledge and support and ensure that Responsible Designers do not have a conflict of interest with the licensee's operations function.

5.49 The licensee must retain sufficient knowledge of all aspects of the design to act as a 'Design Authority Intelligent Customer' to enable it to understand the results of the Responsible Designers' work, and to understand the implications of that work for the life of the plant.

5.50 The licensee should have a strategy to anticipate the possible disappearance of some of the Responsible Designers and contingency plans to manage this situation should it arise.

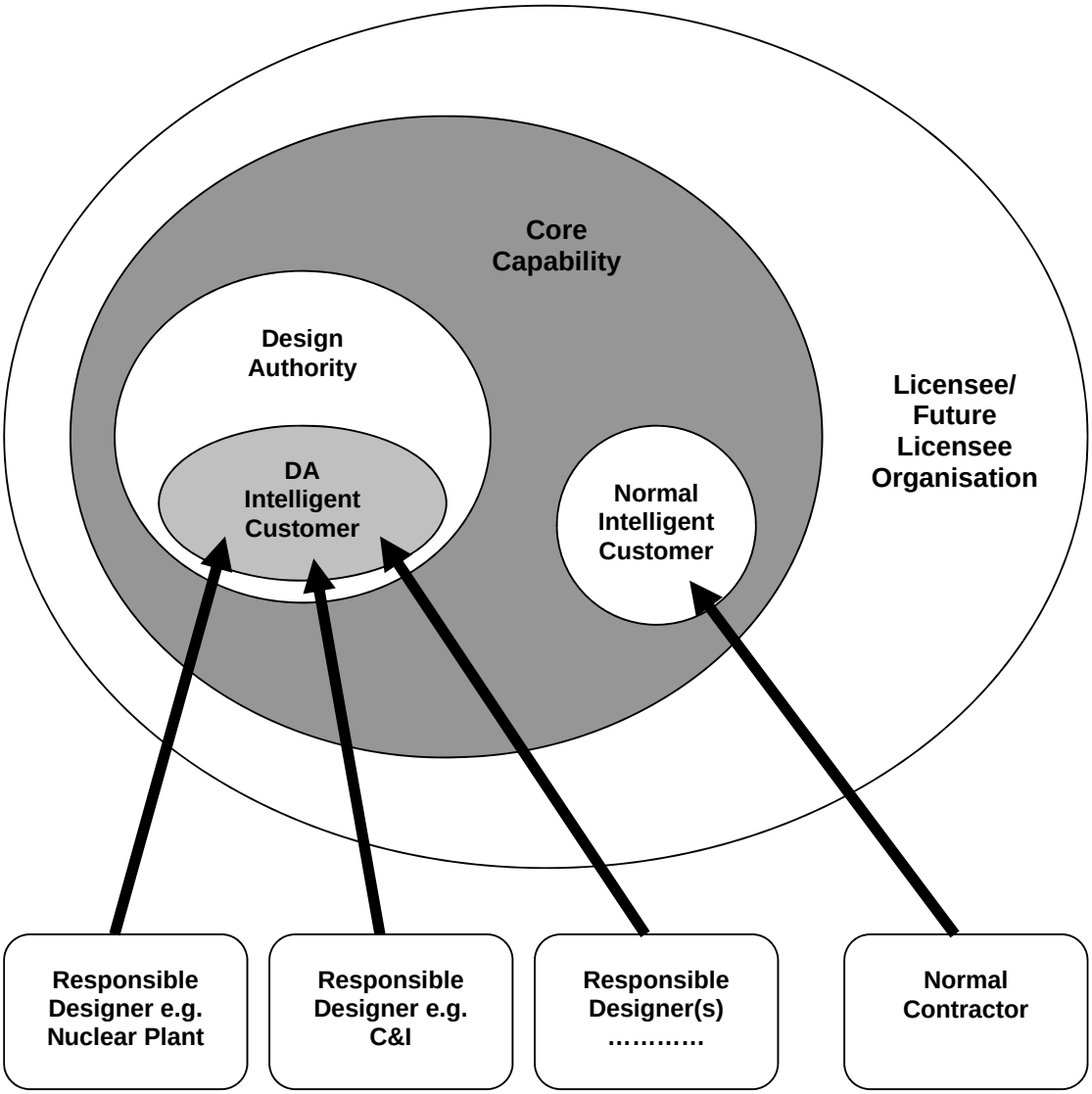
The Inspector should consider whether or not:

- Formal contractual arrangements are in place with individual Responsible Designers to safeguard access to their specialist skills, knowledge and resources;
- The Design Authority is able to demonstrate how it discharges its functional responsibilities with Responsible Designers across the contractual boundaries;

- The contractual arrangements ensure that Responsible Designers maintain their specialised knowledge of design and their competence in their field of expertise;
- The interface/management arrangements with Responsible Designers are clear and ensure that the Design Authority cannot be by-passed i.e. by Responsible Designers liaising directly with plant operators or maintenance/engineering or vice versa;
- There a specialist Intelligent Customer capability within the Design Authority;
- The Design Authority Intelligent Customer is able to demonstrate that it has sufficient knowledge of the design to enable it to understand the results of Responsible Designers' work;
- Arrangements are in place to safeguard access to Responsible Designers' knowledge in the event that this knowledge potentially becomes unavailable over time i.e. through insolvency, corporate takeovers/mergers of the Responsible Designer organisation;
- The quality of Responsible Designers' input to the Design Authority is measured and monitored i.e. using key performance indicators.

6. APPENDICES

APPENDIX 1 – RELATIONSHIP BETWEEN LICENSEE/FUTURE LICENSEE ORGANISATION, CORE CAPABILITY, DESIGN AUTHORITY, DESIGN AUTHORITY INTELLIGENT CUSTOMER AND RESPONSIBLE DESIGNERS



Note: In nuclear safety management for submarine reactors or nuclear warheads the Design Authority service is provided by a central body contracted to MoD to several licensees/authorisees.

APPENDIX 2 – DESIGN KNOWLEDGE REQUIRED BY A DESIGN AUTHORITY

6.1 The Design Authority should have the following knowledge as a minimum:

- A detailed understanding of why the design is as it is;
- The experimental and research knowledge on which the design is based;
- The design inputs such as basic functional requirements, performance requirements, safety goals and safety principles, applicable codes, standards and regulatory requirements, design conditions, loads such as seismic loads, interface requirements etc;
- The design outputs such as specifications, design limits, operating limits, safety limits, failure or fitness for service criteria;
- A detailed knowledge of the design calculations which demonstrate the adequacy of the design and the ability to reproduce the design calculation if needed[4];
- An understanding of the inspections, analysis, testing, computer code validation and acceptance criteria used by participating design organisations to verify that the design output meets the design requirements;
- The assumptions made in all the steps above, including assumptions related to operating modes or procedures, expected life history;
- The implications of operating experience on the design.

[4] This will normally be delivered by a close contractual relationship with and oversight of the Responsible Designer. Where a Responsible Designer is not the original plant designer, the Design Authority should take special care to verify its competence to fulfil this role.