WORLD NUCLEAR ASSOCIATION

Implementation of the Design Authority Within a Nuclear Operating Organization

A supplement to the CORDEL report "Design Knowledge and Design Change Management in the Operation of Nuclear Fleets"

Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group

Title: Implementation of the Design Authority
Within a Nuclear Operating Organization
Produced by: World Nuclear Association
Published: March 2017
Report No. 2017/003

Contents

1 Executive Summary

This document is intended to describe some of the principles of a nuclear operator's Design Authority. These were introduced in the report "Design Knowledge and Design Change Management in the Operation of Nuclear Fleets", published by the World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group [1].

While based largely on US experience, it provides a useful reference regarding the implementation of a Design Authority within different operating organizations. Other experiences regarding various countries are also taken into account, as recommended in the earlier CORDEL report.

Since the licensee is the entity that is responsible for the safe operation of the facility and for protecting the health and safety of the public, it is clear that the Design Authority must be in the licensee's organization. The International Atomic Energy Agency (IAEA) Safety Standard SSR-2/1 [2] stipulates: "The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant," which is consistent with the concept of Design Authority defined in IAEA INSAG-19 [3].

There have been many definitions of the role of the Design Authority in various standards and documents on configuration management. The responsibilities of a Design Authority proposed in this document are:

- Obtaining design basis information from external or internal organizations.
- Reviewing the adequacy of the design assumptions and attributes in the design basis in the light of new information arising from operating experience, new research findings, new analytical findings, and potential changes to the range of conditions and events.
- Maintaining the integrity of the design basis and controlling changes that may affect it.
- Development, implementation and control of the design change process.
- Approving changes to the plant configuration.
- Ensuring that the plant configuration is in accordance with the facility's design basis and licensing basis.
- Ensuring that plant procedures, including operating and emergency procedures, are consistent with the plant's design and licensing bases and reflect the current plant configuration.
- Ensuring that proposed changes to the plant's design do not inadvertently change the plant configuration and/or documentation in such a way that would violate the design assumptions or design attributes relied on to mitigate design and beyond design basis accidents[1].

One of the fundamental prerequisites for establishing a Design Authority is that the licensee must be a 'knowledgeable customer', throughout the lifetime of the plant, from construction to operation and decommissioning. Some of the key attributes of a knowledgeable customer include:

- Understanding the plant's design and licensing bases and changes being made to the facility that may affect these.
- Being actively involved in, and taking ownership of, changes to the facility in which modifications are performed by authorized organizations.

[1] Beyond design basis events are referred to by the IAEA as "design extension conditions". See IAEA SSR-21-1, Safety of Nuclear Power Plants: Design [2].

- Maintaining a working relationship with the nuclear steam supply system (NSSS) vendor, the architect-engineer and other entities that participated in the original facility design and significant plant modifications.
- Maintaining an awareness of industry experience and assessing its applicability to the facility.

Since changes to plant configuration affect not only the design of the plant but may also affect plant operation, the Design Authority function should be embodied in an entity reporting to senior management (such as a vice president at plant level, or executive vice president at corporate level). Furthermore, since plant modifications can affect not only the design and licensing bases but also plant operating procedures, the Design Authority function must be multi-disciplined. The Design Authority should comprise experts in engineering disciplines such as instrumentation and control, mechanical, electrical, and civil engineering, as well as representatives from the plant operating staff, plant system engineers, safety engineers and licensing engineers.

Since a nuclear plant will operate for 40 years or more, its operating lifetime likely exceeds the working careers of its staff and also staff at the NSSS vendor and other design organizations that participated in the initial plant design and construction. The Design Authority should ensure that there is a transfer of knowledge in all these organizations such that the design and licensing bases will be retained over the lifetime of the plant.

2 Introduction

The report, "Design Knowledge and Design Change Management in the Operation of Nuclear Fleets" [1], prepared by the World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Design Change Management Task Force points out the importance and challenges of controlling the plant configuration throughout the plant's entire lifetime. Such challenges include: the operating lifetime of a plant will likely extend beyond the working careers of the plant staff; and the design information received by the licensee of the plant may not be sufficiently detailed, particularly for plants constructed and sold under a turnkey contract, such that an accurate point of departure for plant modifications cannot be firmly established from the documentation provided by the NSSS vendor or the architect-engineer.

In addition, there are issues of a proprietary nature. Typically, a licensee purchases the plant and the information necessary to operate it safely but not the plant's design. This proprietary design information, such as the computer models used in evaluating the consequences of design basis accidents, or the design analyses that demonstrate the integrity of the reactor coolant system pressure boundary and components are usually retained by the NSSS vendor. This necessitates the need to retain the NSSS vendor to perform or be involved with certain plant modifications or normal fuel reloading, which entails re-performing the accident analyses for the new core configuration. Clearly, there are many challenges facing the licensee in establishing, understanding and maintaining configuration control, such that the plant can be operated in a safe manner throughout its lifetime.

The topic of Design Authority is discussed in IAEA INSAG-19, "Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life" [3]. Consistently, IAEA SSR-2-1, "Safety of Nuclear Power Plants Design" [2], requires establishing and implementing "a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant, within the operating organization." The Western European Nuclear Regulators Association (WENRA) document "Safety Reference Levels for Existing Reactors" [4] also discusses specific requirements related to the concept of Design Authority. And the World Association of Nuclear Operators (WANO), in its "Principles for Design Basis Management" [5], requires the establishment of a Design Authority for design basis and beyond design basis management. It also lists the attributes of the Design Authority.

This CORDEL report is intended to give practical insights into Design Authority, its attributes and some challenges in establishing and maintaining it.

3 INSAG-19 and SSR-2/1

INSAG-19 [3] is a high-level report which has been prepared by an advisory group for the IAEA Director General and is aimed at senior utility executives who are responsible for the overall safety of nuclear installations. It has been used as a basis for the elaboration of the Specific Safety Requirements IAEA SSR-2/1 "Safety of Nuclear Power Plants: Design" [2] which is one of the IAEA Safety Standards. It emphasizes the need to maintain design integrity over the operating lifetime of the facility and provides guidance for establishing within the licensee organization an organization referred to as the Design Authority, which has three primary areas of responsibility (see paragraph 12 of INSAG-19):

- The design process.
- Approval of design changes.
- Ensuring that requisite knowledge is maintained.

The terms 'design intent' and 'maintain design integrity' are used in INSAG-19. Although INSAG-19 does not define the term "design intent", it uses it in two places:

Paragraph 5

> "Nuclear power plants are complex machines. They are composed of many interdependent systems which must operate in a manner that meets the design intent over a period of many decades."

Paragraph 10

> "The operating organization must also assure itself that a formal and rigorous design change process exists so that the actual configuration of the plant throughout its life is consistent with changes to the design, that changes can be made with full knowledge of the original design intent, the design philosophy and of all the details of implementation of the design, and that this knowledge is maintained or improved throughout the lifetime of the plant."

The main point is that the plant licensee must maintain and be knowledgeable of the plant's design and licensing bases, over the operating lifetime of the plant. It is recognized that the design basis of an SSC may change over the course of plant operation requiring the approval of the regulator for changes that affect plant safety or that of the Design Authority for non-safety-related changes. The concept of 'design intent' is incorporated within the design basis.

In many instances in INSAG-19 the term 'maintain design integrity' is used. For example in paragraph 10, it states:

> "The need to maintain design integrity and to preserve the necessary detailed and specialized design knowledge poses a significant challenge for the organization that has overall responsibility for the safety of a plant over its operating lifetime."

The use of the phrase 'maintain design integrity' is not defined in INSAG-19, but it can be inferred that the meaning is to maintain the plant configuration in accordance with its design and licensing bases.

4 Definitions

The holder of an operating licence for a nuclear power plant is responsible for the overall safety of the plant and for protecting the health and safety of the public (see IAEA Fundamental Safety Principles [6]). It follows that, since the control of plant modifications has a direct bearing on the ability to operate the nuclear plant safely and in accordance with the terms and conditions of its licence, the responsibility for controlling the plant's configuration rests with the licensee. Therefore, the Design Authority, *i.e.* the entity responsible for gathering and maintaining the plant's design basis and controlling the plant's configuration and changes to the configuration must also be within the licensee's organization.

Design Authority

IAEA INSAG-19 defines Design Authority as: "The designated entity that takes the overall responsibility for the design process, approval of design changes, and for ensuring that the requisite knowledge is established, preserved and extended with experience."

Although not explicitly defined in IAEA SSR-2-1 or the IAEA Safety Glossary [7], other definitions exist for Design Authority. One such definition is in ASME NQA-1 [8], which defines Design Authority as: "The organization having the responsibility and authority for approving the design bases, the configuration, and changes thereto."

The United States Nuclear Regulatory Commission (NRC) in NUREG-1397 [9] defines Design Authority as "The organization having responsibility for maintaining the design bases and ensuring that design output documents accurately reflect the design bases."

WENRA Safety Reference Levels for Existing Reactors [4] mentions the following requirement: "The licensee shall always have in house, sufficient, and competent staff and resources to understand the licensing basis of the plant (*e.g.* Safety Analysis Report or Safety Case and other documents based thereon), as well as to understand the actual design and operation of the plant in all plant states."

Taking this into account, the responsibilities of the Design Authority proposed by CORDEL are as follows:

- Obtaining design basis information from external and internal organizations.
- Reviewing the adequacy of the design assumptions and attributes in the design basis in light of new information arising from operating experience, new research findings, new analytical findings, and potential changes to the range of conditions and events.
- Maintaining the design basis and controlling changes to it.
- Development, implementation and control of the design change process.
- Approving changes to the plant configuration.
- Ensuring that the plant configuration is in accordance with the facility's design basis and licensing basis.
- Ensuring that plant procedures, including operating and emergency procedures, are consistent with the plant's design and licensing bases and reflect the current plant configuration.
- Ensuring that proposed changes to the plant's design do not change the plant configuration and/or documentation in such a way that would violate the design assumptions or design attributes relied upon to mitigate design and beyond design basis accidents.

- Ensuring that requisite knowledge is maintained among appropriate staff members

The terms "Owner" and "Configuration" are important in the context of discussing the Design Authority. CORDEL proposes that these terms are defined, for the purpose of this report, following definitions from the IAEA Safety Glossary and/or ASME NQA-1:

Owner

The organization legally responsible for the construction and/or operation of a nuclear facility including but not limited to one who has applied for, or has been granted, a construction permit or operating licence by the regulatory authority having lawful jurisdiction.

Configuration

The physical, functional, and operational characteristics of the structures, systems and components, or parts of the facility.

Configuration management

The process of identifying and documenting the characteristics of a facility's structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation.

Responsible Designer

INSAG-19 [3] introduces the term 'Responsible Designer' but does not provide an explicit definition. The following definition is proposed for Responsible Designer:

An organization contracted or formally designated by the licensee to design plant modifications. The Responsible Designer will likely be the organization responsible for that portion of the plant design being modified.

Given that the licensee has the legal responsibility for construction and safe operation of the nuclear plant, it follows from the above definitions that the organization having the responsibility for configuration management must be with the entity designated as the Design Authority within the licensee's organization.

While the licensee is legally responsible for the safe operation of the nuclear facility, in many instances it would be difficult for it to have the level of technical expertise within its organization needed to design and analyze proposed changes or modifications to its facility. This is particularly true in specialty areas such as seismic design or in the reanalysis of postulated accidents that could be affected by changes to systems, structures or components as well as changes to plant operating procedures. It is therefore often necessary for the licensee to delegate certain technical activities to outside organizations. Nevertheless, the licensee cannot delegate the responsibility for plant safety during or after the implementation of any facility changes or modifications.

Section III of the ASME B&PVC recognizes that the Owner may not always have sufficient technical expertise to perform certain activities relating to the design of pressure vessels therefore, the term 'designee' was defined as: "Any organization that performs specified activities at the request of the Owner". The Owner retains the responsibility for the activity performed by the designee.

The term 'designee' in Section III of the ASME B&PV Code is similar to the concept of Responsible Designer defined in INSAG-19. In the context of this report, the term 'designee' relates not only to the design of pressure retaining components but more broadly to other engineering and design activities.

5 Configuration Management

Design Authority is an important aspect of configuration management because it encompasses the necessary control of changes to the plant's configuration to ensure that the plant continues to be aligned with its design and licensing bases and that the integrity of the design basis is met and maintained.

Each nuclear facility has its own defined design basis which must comply with and meet the appropriate regulatory requirements.

The IAEA, in its Safety Glossary (draft edition 2016), defines 'design basis' as: "The range of conditions and events taken explicitly into account in the design of structures, systems and components and equipment of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits."

It is important to note from the above definition that the functional goals for structures, systems and components are derived from the analysis of postulated accidents. Therefore, any changes to structures, systems and components need to be carefully controlled throughout the lifetime of the facility to maintain the integrity of the plant's design basis, and the conformance to safety and regulatory requirements, as well as to the licence conditions imposed by the operating licence or safety demonstration (for example the conformance with technical specifications, which are usually part of the operating licence). In some instances, a plant modification could put the facility outside its design basis. In this case, regulatory approval would be necessary prior to implementation of the plant modification.

For regulation in the US, 'design bases' is also an important term. It denotes that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (a) restraints derived from generally accepted "state-of-the-art" practices for achieving functional goals; or (b) requirements derived from analysis (based on calculations and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals.

In addition to the facility's regulatory design basis defined above there is also – essentially in the US - an engineering design basis. This is defined (as engineering design bases) in NUREG-1397 as: "The entire set of design constraints that are implemented, including those that are (1) part of the current licensing bases and form the bases for the staff's safety judgements and (2) those that are not included in the current licensing bases but are implemented to achieve certain economies of operation, maintenance, procurement, installation, or construction".

For example, the heat removal capacity of the residual heat removal system in a pressurized water reactor is directly proportional to the time that is required to cool the reactor coolant system before fuel loading operations can begin. This is an economic rather than a regulatory consideration in that the more quickly fuel loading operations can be completed, the less time the plant is offline. Therefore, increased heat removal capability of the residual heat removal system can translate to shorter plant reloading outages.

The main point is that to properly manage the plant configuration, the Design Authority and the

Responsible Designer need to understand not only the regulatory bases for granting of the operating licence but also any design features that may affect the economical operation of the plant. In addition, the Design Authority or the Responsible Designer should clearly establish the point of departure for plant modifications such as the calculation basis for system design and sizing of equipment and any important calculation assumptions.

In the late 1980s and early 1990s, the NRC's inspection program found examples where plant modifications had not been properly controlled and vetted such that the plant's design bases had been compromised. This resulted in a commission policy statement, "Availability and Adequacy of Design Bases Information at Nuclear Power Plants" [10]. This policy statement emphasized the importance of maintaining conformance with the facility's design basis. During this time, many facilities initiated design basis reconstitution programs which were costly and time-consuming, further emphasizing the need for the designation of a Design Authority as a part of a configuration management program The loss of configuration control resulted not only in safety concerns raised by not maintaining conformance with the plant's design basis that needed to be addressed by some licensees but also the economic penalty for the licensees in having to reconstitute their facility's design basis and to ensure conformance to it.

The WENRA Safety Reference Levels for Existing Reactors [4] mention the following requirements related to configuration management: "The licensee shall ensure that no modification to a nuclear power plant, whatever the reason for it, degrades the plant's ability to be operated safely. The licensee shall control plant modifications using a graded approach with appropriate criteria for categorization according to their safety significance."

6 Methods for Establishing and Maintaining Control of the Plant Configuration

The overarching and starting principle is that the licensee should be a 'knowledgeable customer'. This is important for two reasons: first, the licensee is responsible to the regulatory authority for safe operation of the nuclear plant and protection of public health and safety; second, the licensee has made a substantial financial commitment in the construction of a nuclear power plant and operating the plant safely and efficiently protects its investment. In the USA, there have been several instances where loss of plant configuration has resulted in extended shutdowns. These regulatory enforced shutdowns (sometimes several years in duration) were very costly and could have been avoided had the licensees had effective configuration management programs.

A licensee's comprehension of the plant's design basis should begin as soon as possible after the award of the contract with the NSSS vendor. In order to maintain the integrity of the plant's design basis throughout the plant's operating lifetime, the licensee first needs to have a thorough understanding of the plant's design basis, as this will be the point of departure for future plant modifications.

One way that the licensee can gain an understanding of the plant's design basis is through designating engineers, perhaps one for each technical discipline (mechanical, electric power, instrumentation and control systems, etc.), to interface with both the NSSS vendor and other design organizations, such as the architect-engineer, early on in the construction process. In this way, the knowledge transfer process can begin.

The concept of system engineers is common in operating plants. In an operating plant, the system engineer is the person most knowledgeable of their assigned system and should review all modifications before implementation to assure that the system will continue to meet the plant's design basis. Identifying system engineers early in the construction process will facilitate the knowledge transfer from the NSSS vendor and the architect-engineer to the Design Authority. Furthermore, the system engineer should also be thoroughly familiar with normal, abnormal and emergency operating procedures for their system. In this regard, it would also be useful for the system engineer to participate, if possible, in the initial development of these procedures.

As the plant transitions from construction to operation, it is important for the licensee to obtain sufficient documentation from the NSSS vendor and the architect-engineer to have a record of the design basis for systems, structures and components in its respective scopes. This should include documents necessary for design basis and beyond design basis knowledge and establishment, normal and emergency operating procedures, testing procedures and test results, equipment qualification reports, maintenance guides, calculation models, as well as acceptance criteria with

demonstration of their level. The provision of this information should be considered during the contractual stages and may be included in the scope of the contracts between the licensee and principal design organizations. Some information may be difficult to obtain due to proprietary considerations.

The participation of a licensee in the owners group for facilities of similar design may prove beneficial in obtaining information from the NSSS vendor.

During the operating lifetime of the nuclear facility, there will no doubt be changes to the plant. These changes will either be driven by the desire to facilitate plant operation (such enhancements may be identified over the course of plant operation), upgrade to new technology, particularly in the area of computer-based systems, or address a safety issue (generally resulting from the operating experience at national or international level). Whatever the reason for the change, it is important for the licensee to understand the technical aspects of the changes made and their effect, if any, on the plant's design basis. This is particularly important when the changes are designed by external organizations, such as a Responsible Designer.

A licensee will have some degree of engineering expertise on its staff. The amount of expertise will vary according to the size of the organization and the number of plants that the licensee operates. While the licensee will have some capability to make physical changes to the plant, there are certain changes that require very specialized expertise where the licensee will have to contract these to a Responsible Designer. These areas may be changes to the NSSS, revision of safety analyses for new core configurations following fuel reloading, structural changes to the facilities, reanalysis of piping systems following installation of new equipment and seismic reanalysis of structures and systems are some examples of more technically complex areas that may be contracted out.

As stated earlier, the licensee can contract out activities but not the responsibility for safety. Therefore, the licensee is responsible for plant modifications designed and implemented by other organizations. In this regard, such contracted plant modifications present an opportunity for the licensee to acquire knowledge by interacting with the original designer. For such modifications, it would be advisable for the licensee to have one or more engineers, depending on the complexity of the modification and the number of technical disciplines involved, to work with the Responsible Designer to understand the details of the modification, the methodology of the analyses as well as any assumptions made. Such involvement will also provide the licensee with further insights into the plant's design basis.

The key to being a knowledgeable customer is obtaining and understanding as much information as possible regarding the plant's design basis. This should begin early in the construction process and continue over the course of the plant's operating lifetime. This knowledge is vital to the function of Design Authority.

7 Responsibilities of the Design Authority

7.1 Establishment of the Design Authority

Senior management at each nuclear power plant or nuclear fleet should establish a functional group that has the responsibility for the management of the plant configuration and changes to the facility's configuration to ensure that the facility meets its design and licensing basis. If a licensee has several operating nuclear power plants, it should ensure that each plant has a Design Authority, either on site or at corporate level. If the licensee operates two or more similar facilities, it should consider establishing a Design Authority at the corporate level that has the responsibility of ensuring that these facilities maintain their similarities. Doing this is important to safety because generic safety issues may be addressed in a similar manner across these plants. Furthermore, from an operational point of view, maintaining similarity between facilities makes it easier to move personnel between sites. It can also help to ensure that modifications made to improve staff capability or nuclear safety, or to operate the facilities more efficiently, can be shared between similar facilities in the fleet.

The designated Design Authority at a given site should report to a senior plant manager, such as the director of engineering, or a site nuclear vice president. The composition of the Design Authority should include lead engineers in the civil, mechanical, electrical, and instrumentation and control disciplines who are knowledgeable of the facility's design basis. Since many plant modifications involve one or more disciplines, inter-disciplinary involvement is vital. The Design Authority should also include a representative from the operations staff, *e.g.* a shift supervisor, shift technical adviser or senior reactor operator since potential modifications may affect plant operation or require changes to be made to normal, abnormal or emergency operating procedures. Members of the Design Authority should also include a licensing engineer, a safety engineer and the system engineer for the system being modified to ensure that the integrity of the plant's design and licensing bass are maintained. A representative from the plant maintenance organization should also be a member of the Design Authority as plant modifications may affect maintenance and test procedures.

7.2 Duties and Responsibilities of the Design Authority

The Design Authority is responsible for the management of the plant configuration to ensure that any changes to the configuration do not put the plant outside its design basis and the conditions of its operating licence.

The duties of the Design Authority should include maintaining the integrity of the plant's design basis, and reviewing and approving any change to the plant configuration to verify that these changes are consistent with the facility's design basis and operating licence. Such changes might include: the replacement of components; the addition of new components or plant systems; modifications to existing systems, structures or components; and changes to normal, abnormal or emergency operating procedures.

Examples of the duties and responsibilities of the Design Authority are those of the plant operations review committee (PORC) in US plants (see Appendix). Establishment of the PORC is a requirement of the operating licence for US plants, where it may

be possible to have the PORC designated as the Design Authority, with some expanded duties and responsibilities, as necessary.

The duties of the Design Authority should include ensuring that:

- The design basis specifies the capabilities of the plant to cope with a specified range of plant states within the radiation protection requirements [4].
- The design basis includes the specification for normal operation, anticipated operational occurrences and design basis accidents from postulated initiating events (PIEs), the safety classification, important assumptions and, in some cases, particular analysis [4].
- The design basis shall regularly, and as a result of operating experience and significant new safety information, be reviewed, using both a deterministic and a probabilistic approach as well as engineering judgement to determine whether the design basis is still appropriate [4].
- As part of defence-in-depth, analysis of design extension conditions (DEC) are undertaken with the purpose of further improving the safety of the nuclear power plant by: enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis; and minimizing radioactive releases harmful to the public and the environment as far as reasonably practicable, in such events or conditions [4].
- The integrity of the plant's design basis is maintained and controlled.
- The conformity of SSCs is guaranteed throughout the lifetime of the plants, in particular considering ageing and obsolescence.
- Activities affecting plant configuration have been performed and verified in accordance with the licensee's quality assurance Program.
- Design interfaces between internal and external organizations have been identified and design information transmitted across interfaces has been controlled.
- Plant changes have been prepared and reviewed by qualified personnel.
- The source of design inputs is documented and the referenced documents reflect up-to-date information.
- All calculation assumptions are identified and justified.
- Final design documents are sufficiently detailed such that a technically qualified person can understand the documents.
- Final design documents reflect the most adverse design conditions in line with the plant's design basis.
- For proposed modifications incorporating the use of commercial-grade parts or components that have been dedicated[2], that traceability of documents supporting the dedication as well as the accreditation of the dedicating organization have been established.
- Where computer-based analysis is used, verification that the computer code has been developed under a quality assurance program that conforms to regulatory requirements.
- Design documents supporting changes to plant configuration have been appropriately verified.
- Inputs to procurement documents have been controlled and verified to reflect the most current design information.
- Procurement documents specify any component qualification requirements, such as seismic and environmental qualification, and the appropriate parameters for

[2] This paragraph relates to the commercial-grade dedication of items for use in safety-related systems, a procedure specifically developed in the US by EPRI [11].

qualification are consistent with the plant's design basis. In addition, the qualifications for components are maintained throughout the lifetime of the plant.

- Procurement documents specify quality requirements and any regulatory reporting requirements.
- Plant procedures affected by the change to plant configuration have been identified and any required procedural changes have been implemented before the new/revised SSC has been put into service.
- Changes to the final design, non-conformances or inconsistencies to design or installation documentation, or necessary on-the-field changes have been identified and reconciled with the design documents or procedures.
- Temporary changes to plant configuration, sometimes referred to as 'work arounds', are reviewed periodically to determine if these have been reflected in plant procedures and continue to be necessary or whether permanent plant modifications need to be considered.
- Plant operating experience and plant modifications are shared with the appropriate plant owners group.

It is also important that the Design Authority maintains a close relationship with the NSSS vendor and the other significant design organizations involved in the original design, such as the architect-engineer. This is beneficial to obtaining design basis information. Furthermore, the NSSS vendor may have identified possible modifications to the plant design based on operating experience at similar facilities or through research performed to support enhanced designs. These modifications should be evaluated by the Design Authority for possible incorporation into the plant.

Since nuclear power plants will operate for 40 years (or more with licence extension or after periodic safety reviews), the facility's lifetime is likely to exceed the working careers of its staff and also staff at the NSSS vendor and other design organizations that participated in the initial plant design and construction. A challenge for the Design Authority will be to ensure that that there is a transfer of knowledge in all these organizations such that the design and licensing bases will be retained over the lifetime of the facility.

Most, if not all, NSSS designs have owners groups. These groups provide a forum for sharing operational experience between the licensees of different plants but similar facilities. A designated member of the Design Authority should participate in owners group meetings.

7.3 The Responsible Designer and the Interface With the Licensee and the Licensee's Design Authority Organization

As previously defined of this report, the Responsible Designer is an organization that is contracted or identified within the operator's organization to design and possibly perform installation or modifications to the plant's configuration. Typically, the designated Responsible Designer will be the organization that is responsible for the original design of the plant being modified. For example, the NSSS vendor would be the likely Responsible Designer for modifications to the reactor coolant system, reactor protection system, in-core and external nuclear instrumentation, core configuration, and the plant's safety analyses to support the core configuration during fuel reloading. The architect-engineer would typically be the Responsible Designer for modifications to structures, routing and analysis of piping systems and pipe supports, the safety and non safety-related electric power distribution system, plant instrumentation and control systems not part of the NSSS vendor's scope of supply, emergency diesel generators, design and routing of electrical cable trays and electrical conduits, and design of the secondary plant. This, of course, varies depending on contractual agreements that are plant-specific. However, this may not always be the case, as the Responsible Designer may not be the original designer. If the Responsible Designer is not the entity that performed the original design of the SSC being modified, this requires significantly more involvement of the Design Authority than if this were not the case, as discussed below.

7.3.1 Interface Between the Design Authority and the Responsible Designer When the Responsible Designer Performed the Initial Design

If the Responsible Designer is the same party that designed the original SSC, it is likely that it will have the original design basis for the SSC that is being modified, though this should be verified by the Design Authority. Prior to awarding the contract for the modification, representatives of the Design Authority of the relevant technical disciplines should meet with the Responsible Designer to discuss the proposed modification and to gain an understanding of the design basis that will form the constraints within which the modification needs to conform. This may also provide additional insight into aspects of the design basis that may not be well understood by the Design Authority.

As previously stated, the licensee is responsible for maintaining the integrity of the plant's design basis

and conformance between the facility configuration and the design and licensing bases whether the modification is contracted out or performed in-house. Therefore, the Design Authority should participate to the fullest extent possible in any contracted modification and should carefully review and approve the modification package prior to its implementation to ensure the integrity of the plant's design basis is maintained. This review should include:

- Verifying that the quality assurance program of the Responsible Designer is consistent with the licensee's quality assurance program.
- Verifying that the scope of the modification is consistent with the contract.
- Verifying that the design basis for the modification has been identified and documented in the modification package to provide traceability to the source documents.
- Reviewing all analysis to verify:
  - Design interfaces between involved technical disciplines have been established and controlled.
  - Design inputs are traceable to design basis documents.
  - The appropriateness of the computing methodology.
  - Computer programs used for analysis have been benchmarked against known results, validated, meet specified quality assurance requirements and are acceptable to the regulatory authority.
  - Computing assumptions are reasonable and have been appropriately justified.
  - Reasonableness of computing results.
  - Analyses and calculations have been verified in accordance with the Responsible Designer's quality assurance/design control program.
  - The completed modification meets the design and licensing bases and that any instances where the design basis or licensing basis cannot be met are identified; and the approval of such changes to the design bases are approved by the Design Authority and approved by the regulatory body prior to implementation of the modification.
- Verifying that plant documents, *e.g.* drawings and procedures, which needed to be updated as a result of the modification, have been identified and the appropriate changes have been made.
- Verifying that materials used meet the design code of record and are suitable for the intended use and environment.
- Verifying that design information is controlled and accurately reflected in procurement documents, including equipment qualification requirements (such as seismic and environmental requirements).
- Verifying that the technical information provided in procurement documents is consistent with the plant's design basis, prior to going out to tender.
- Verifying that the modification package includes installation procedures and test procedures with specific acceptance criteria.
- If the modification is to be implemented in stages, verification that the plant configuration, with the partially implemented modification, meets the plant's design basis.
- Verifying that the final documentation supporting the modification that establishes the maintenance of the integrity of the plant's design basis is provided to the Design Authority at the completion of the modification.

Even when a plant modification is performed by a Responsible Designer, the Design Authority needs to take ownership of the modification. This means that the Design Authority should have a full understanding of the modification and why it maintains the integrity of the plant's design basis. It is possible that a licensee, particularly one that operates a single facility, might not have expertise within its staff to perform complex analysis such as seismic analysis, complex stress analysis, or thermo-hydraulic analysis. However, the licensee should have sufficient technical expertise on its staff to review for acceptance the modifications performed by a Responsible Designer.

7.3.2 Interface Between the Design Authority and the Responsible Designer When the Responsible Designer did not Perform the Initial Design

If the Responsible Designer is not the entity that performed the original design for the plant SSC that is being modified, it then becomes the responsibility of the Design Authority to provide the Responsible Designer with information required to prepare the modification in a manner that conforms to the plant's design basis. The information provided should include:

- The design and licensing bases pertinent to the proposed modification, particularly those that may need to change.
- Analysis required to support changes to the design basis.
- Safety class of the system being modified.
- Identification of any industry codes and standards to be used.
- Any physical constraints, interferences or special requirements that need to be accommodated in the proposed modification.
- System descriptions.
- Piping and instrumentation diagrams.
- Plant layout drawings showing the location of components and routing of piping and cable trays and electrical conduits.
- Plant maintenance and test procedures that are affected or may be affected by the proposed modification.
- Seismic and environmental equipment qualification requirements.

Control of the plant's configuration to maintain consistency with the plant's design and licensing bases is of paramount importance and this responsibility falls on the Design Authority. Where the Design Authority does not have the relevant design basis information, it needs to go back to the original designer to obtain this information, if possible. If it is not possible to obtain the design basis information, the Design Authority needs to reconstitute the design basis information using the information it has available or by performing its own calculations and analysis to determine the design basis. A modification should never be made to a plant without a complete and full understanding of the design basis applicable to the proposed modification and how the modification conforms with the design basis.

The duties and responsibilities of the Design Authority where the Responsible Designer is not the original designer are identical to those described in Section 7.3.1; however, the Design Authority should oversee more closely the modification being implemented by the Responsible Designer.

8 Implementation of the Design Authority Within Different Organizational Structures

The implementation of the Design Authority function may vary with different organizational structures. It is up to each entity to set up the appropriate organization to address its main objectives. The organizational structures considered include:

- A licensee that operates a single unit.
- A licensee that operates multiple similar units at a single site or multiple sites.
- A licensee that operates dissimilar units at a single site or multiple sites.

It is possible to group together the first and third of these organizational structures since they must have a separate Design Authority for each facility. For the second structure, it may be possible to have a centralized Design Authority if the plants are sufficiently similar. This may be advantageous as this should lead to some economies of scale.

However, having one central Design Authority can be very complicated. Similarity does not necessarily mean that the units are identical. The greater the divergence of the units the more differences there are likely to be in their design and licensing bases. Obvious differences are site-related design bases, such as seismically-induced ground motions, or means of communication with the ultimate heat sink. Further, while the units may have similar NSSSs, they may have had different architect-engineers, which could introduce differences between the units, for example functionally similar components could be supplied by different vendors. The licensee would need to evaluate the additional complexities that may be imposed on a centralized Design Authority due to such differences in the plants' design bases and determine whether it is appropriate for its organization. If the units are identical, then having a centralized Design Authority is an easier decision. The greater the differences between units, the stronger will be the tendency towards having a Design Authority for each unit.

9 Concluding Remarks

Several documents that address Design Authority and Configuration Management have been developed by the IAEA and other regional organizations (NRC in the USA, WENRA in Europe).

These documents are comprehensive, but are written at a high level. The current report presents in a more detailed manner, as examples of implementation (not as guidance), the duties and responsibilities of the Design Authority, based on experiences in several countries.

This report is intended to promote the sharing of experience in establishing and maintaining a Design Authority within the operating organizations, between the operators and within operator organizations (WANO and the owners groups) as well as within relevant international organizations and events.

References

[1] Design Knowledge and Design Change Management in the Operation of Nuclear Fleets, World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group, April 2015

[2] IAEA Safety Standards, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1, International Atomic Energy Agency, 2016

[3] Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, A report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, 2003

[4] WENRA Safety Reference Levels for Existing Reactors, Reactor Harmonisation Working Group (RHWG) of the Western European Nuclear Regulators Association, September 2014

[5] WANO Principles for Design Basis Management, PL-2015-1, March 2015 (available for WANO members only)

[6] IAEA Safety Standards, Fundamental Safety Principles, Safety Fundamentals No. SF-1, International Atomic Energy Agency, 2006

[7] IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2007. Edition, International Atomic Energy Agency

[8] ASME NQA-1 Quality Assurance Requirements for Nuclear Facility Applications, 2015

[9] NUREG-1397, An Assessment of Design Control Practices and Design Reconstitution Programs in the Nuclear Power Industry, US Nuclear Regulatory Commission, February 1991

[10] 10 CFR Part 50, Availability and Adequacy of Design Bases Information at Nuclear Power Plants, 57 FR 35455, August 10, 1992

[11] EPRI Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications, rev. 1 to EPRI NP-5652 and TR-102260, September 2014

Abbreviations

ASME	American Society of Mechanical Engineers
ASME B&PV Code	American Society of Mechanical Engineers Boiler and Pressure Vessel Code
NSSS	Nuclear steam supply system
PORC	Plant Operations Review Committee (an entity within nuclear plants operating organizations in the USA)
SSCs	Structures, systems and components
WANO	World Association of Nuclear Operators
WENRA	Western European Nuclear Regulators Association
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Group – a group of experts with high professional competence in the field of safety working in regulatory organizations, technical support organizations, research and academic institutions and the nuclear industry. INSAG is convened under the auspices of the IAEA with the objective of providing authoritative advice and guidance on nuclear safety approaches, policies and principles. In particular, INSAG will provide recommendations and opinions on current and emerging nuclear safety issues to the IAEA, the nuclear community and the public.
CORDEL	Cooperation in Reactor Design Evaluation and Licensing – a World Nuclear Association working group

Appendix I | Excerpt from WANO Principles for Design Basis Management

Nuclear safety depends on the operator's ability to manage, understand and challenge the design basis and beyond design basis throughout the life of the plant. In the past, operating experience has shown that shortcomings in these areas have resulted in significant and even catastrophic events, most notably at Fukushima Daiichi in March 2011.

Based on these considerations, the following principles for design basis and beyond design basis management have been established […]:

1. The design authority is established and supported by processes that define authorities, responsibilities and accountabilities for staff and organizations taking part in design-related activities.

2. The design basis is clearly defined, documented, controlled and retrievable.

3. Design limits and operating margins are defined, understood and managed.

4. The adequacy of the design assumptions and attributes in the design basis is reviewed in light of new credible information arising from operating experience, new research findings, new analytical findings, and potential changes to the range of conditions and events.

5. As part of defense-in-depth, processes exist to identify, evaluate and, where appropriate, mitigate the consequences of credible beyond design basis considerations.

6. Appropriate staff members have awareness and understanding of the design basis and beyond design basis considerations, such that the plant configuration and/or documentation is not inadvertently changed in such a way that would violate the design assumptions or design attributes.

Appendix II

Typical Duties of the Plant Operations Review Committee at US Nuclear Plants

- Review of all administrative procedures.
- Review of the safety evaluations for: (1) proposed procedures and instructions; (2) changes to procedures and instructions, equipment, systems or facilities; and (3) tests or experiments performed to verify that they are not outside the design bases.
- Review of proposed procedures and instructions and changes to procedures and instructions, equipment, systems or facilities which have the potential putting the plant outside its design bases.
- Review of proposed tests or experiments to verify that these do not put the plant outside its design bases.
- Review of proposed changes to technical specifications or the operating licence.
- Investigation of all violations of the technical specifications and actions to prevent recurrence.
- Review of all events reportable to the regulator.
- Review of the plant security plan and security contingency instructions.
- Review of the emergency plan and implementing instructions.
- Review of changes to the offsite dose calculation manual, and radwaste treatment systems.
- Review of any accidental, unplanned or uncontrolled radioactive release recommendations, and disposition of the corrective action to prevent recurrence.
- Review of the fire protection program and implementing procedures.

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org

The World's Nuclear Association's **Cooperation in Reactor Design Evaluation and Licensing** (CORDEL) Working Group promotes a worldwide nuclear regulatory environment where internationally accepted standardized reactor designs can be widely deployed without major design changes at the national level. In practice, this would mean that generic design certification and safety evaluations approved by a recognized competent authority in the country of origin would be acceptable in other countries.

This report entitled **Implementation of the Design Authority within a Nuclear Operating Organization** complements and illustrates some of the principles which are presented in the earlier CORDEL report entitled "Design Knowledge and Design Change Management in the Operation of Nuclear Fleets".

The **World Nuclear Association** is the international organization that represents the global nuclear industry. Its mission is to promote a wider understanding of nuclear energy among key international influencers by producing authoritative information, developing common industry positions, and contributing to the energy debate.