WORLD NUCLEAR ASSOCIATION

Design Knowledge and Design Change Management in the Operation of Nuclear Fleets

Cooperation in Reactor Design Evaluation and Licensing Working Group

Title: Design Knowledge and Design Change Management in the Operation of Nuclear Fleets
Produced by: World Nuclear Association
Published: April 2015
Report No. 2015/002

Contents

Executive Summary

The operating lifetime of a nuclear plant spans several decades. During this time, the plant may undergo design changes as a result of experience feedback, new knowledge or requirements, and safety reviews.

To ensure that safety remains optimised, these changes must be carried out with a full understanding of and without compromising the design intent.

The licensee, usually the operator, holds prime responsibility for the safety of the plant, and by extension it is fully responsible for design change management. According to the IAEA (SSR-2/1), it should fulfil this responsibility by establishing "a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant". This system should include "a formally designated entity responsible for the safety of the plant design within the operating organization's management system", an entity referred to as Design Authority according to INSAG 19, which details its role and responsibility.

The requirement to establish a Design Authority within each nuclear plant operating organization may be challenging. Some of these operating organizations will be new, and some will be small. Some may be the first nuclear operator in a particular country. For plants sold on a turnkey basis, the challenge for the operator to develop and maintain the full knowledge of the design of the plant needed for this role may be greater.

This is the reason why the operator (through its Design Authority) may allocate tasks, under its responsibility, to external organizations that have a specialized knowledge of the detailed design of specific parts of the plant. These organizations are the original designers of the plant, including vendors and equipment suppliers, who have the original design intent knowledge. These external organizations are referred to as responsible designers.

CORDEL's Design Change Management Task Force is investigating options for maintaining design knowledge throughout a plant's lifetime, while also maintaining the benefit of design standardization throughout a fleet.

Based on surveys carried out to substantiate this report (one assessment and comparison of various owners' group practices and one questionnaire to utilities to understand different approaches regarding Design Authority), recommendations are proposed regarding design knowledge and design change management.

Utilities operating plants of similar design, or even more of standardized design, should take advantage of this standardization to manage their design changes. In order to retain this benefit, an international fleet-wide approach to design change management should be seen as a vital concept, because it facilitates a large sharing of experience among operators and enables similar solutions to be adopted for design changes.

There are various mechanisms for managing design changes. The operating organization needs to maintain the underlying design knowledge, while involving the plant's original vendors / designers as needed. Within a standardized fleet, the operator-responsible designer interface over design changes and how they are managed within different organizational and regulatory environments around the world is especially important. This report underlines the importance of a comprehensive cross-involvement of utilities and responsible designers regarding standardized units. The existing opportunities brought by owners' groups, and by other operators' groups such as WANO should be fully developed.

In this context, the nuclear industry may also learn from the aerospace industry's approach to design authority.

1 Introduction

Nuclear development around the world has the potential to bring major benefit for security of supply, energy independence, economic efficiency, environment and high skilled employment. The two main conditions are first the priority to be given to safety in the design and operation of NPPs and second the necessity to reduce the uncertainties in the cost and time of building and licensing new Generation III reactors around the world.

In this context, standardization is a major tool to improve nuclear plant economics during design approvals, licensing and construction, with the potential to bring also significant benefits to operational safety.

The concept of standardized reactor designs does not require units to be completely identical. Rather, all units that use the standardized design technology should at least share the same global architecture and the same specifications for the nuclear steam supply system design and components, and associated safety systems.

In January 2007 the World Nuclear Association (WNA) established the Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group to promote a dialogue between the nuclear industry (including reactor vendors and utilities) and nuclear regulators (national and international organizations) on the benefits and means of achieving a worldwide convergence of reactor safety standards for reactor designs.

CORDEL has produced two reports setting out its mission: i) *Benefits Gained through the International Harmonization of Nuclear Safety Standards for Reactor Designs* [5], and ii) a 'roadmap' report *International Standardization of Reactor Designs* [6]. In both of these, CORDEL argued that, besides economic benefits, international standardization offers an opportunity to make optimal use of best practice and feedback sharing mechanisms and to maximize their contribution to nuclear safety.

As part of a virtuous circle, standardization of nuclear plant design can further facilitate the development of international safety standards, as well as help to reduce uncertainties during licensing and cost overruns during construction. Maintaining the benefit of that standardization all along the fleet's operating lifetime can contribute to performance optimization during operation and decommissioning. This includes the safety performance of the individual units of a worldwide fleet of standardized nuclear plants, which would be expected to be enhanced through mutual sharing of experience and an international fleet-wide approach to design knowledge and design change management.

This report prepared by the CORDEL Design Change Management Task Force (DCMTF) looks at existing and new mechanisms which might deliver improved benefit from design standardization throughout a fleet's lifetime. The main focus of the report is on new-build plants, where the opportunity for standardization is greatest, but some of the recommendations are also applicable to existing fleets.

a) Causes of design change

The operating lifetime of a plant spanning several decades means that it will undergo significant changes during this period. INSAG-19 [1] describes reasons for changes in plant design, such as: physical ageing of structures, systems and components; obsolescence that may occur in hardware and software elements; safety reassessments (for example through periodic safety review (PSR) as required in the EU[1]) and feedback from operating experience; new knowledge and research on safety issues; changing regulatory standards; new best available techniques; and changes

[1] cf IAEA SSG-25 on Periodic Safety Review for Nuclear Power Plants: "It is recognized that some States prefer alternative arrangements to a PSR. For example, some States apply routine comprehensive safety assessment programmes that deal with specific safety issues, significant events and changes in safety standards and operating practices as they arise. Such programmes can, if applied with appropriate scope, frequency, depth and rigour, achieve the same outcomes as the process recommended in this Safety Guide. They allow safety to be improved on a continuous basis and avoid the need to implement concurrently a large programme of corrective actions."

in performance and organizational structure.

A fundamental principle of the nuclear industry is that the operator has prime responsibility for safety [2, 3]; this includes the licensee's ultimate responsibility for the design and design changes. Although the principle of maintaining standardization along the plants' lifetime is important, it is finally up to the operator to decide whether or not to implement design changes that have been carried out at other plants around the world. Reasons for not implementing certain design modifications might be economic, regulatory or due to local conditions (siting *etc*.). Over time, reactors that were originally standardized could therefore become more diverse and the safety and operational benefits of experience feedback could be impaired.

There are several examples where standardized fleets in the nuclear industry have been successfully maintained *e.g.* French fleet, VVER fleet, Westinghouse 4-loop reactors, ABB-CE System 80 plants, GE BWR Mark 4 plants. This experience can also be found in other industries, such as aerospace.

b) The prime responsibility of the operating organization

International discussion and agreement on standardized designs to achieve a similar level of reactor safety across many jurisdictions is under development but still has a long way to go. The processes needed to maintain the benefits of standardization during operation are at an earlier stage of development.

The legal framework in the nuclear industry gives the licensee (*i.e.* the operating organization) prime responsibility for the safety of design and operation. This includes the operator's liability for third-party damage in the case of a nuclear accident. Nuclear power plant design and construction involves many organizations – owner-operators, architect-engineers, nuclear island and balance of plant vendors and designers – and must be adapted to specific site conditions and to regulatory requirements. It creates a large, complex and quite often unique infrastructure project with the operator carrying the overall risk and responsibility for safety.

Regulators currently expect that every licensee maintains a knowledge and understanding of the design that is needed for safe operation, maintenance and modification of every licensed unit. IAEA Safety Standard SSR 2/1 [4] calls for the licensee to maintain design integrity and knowledge within its own organization in "a formally designated entity responsible for the safety of the plant design". INSAG 19 refers to this entity as the Design Authority [1].

The role of the Design Authority is to ensure that:

- The knowledge of the design that is needed for safe operation, maintenance and modification of the plant is available, and maintained up to date by the operating organization;
- The design requirements and the configuration control are maintained throughout the plant's lifetime;
- Interfaces with responsible designers and other organizations engaged in design work are established and controlled;
- The necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization;
- All design changes to the plant are reviewed, verified, documented and approved.

This implies that much of the design knowledge is transferred by the original vendor(s) and designer(s) to the operating organization through safety reports and adequate detailed engineering documentation. However, much of the highly specialized knowledge - *e.g.* codes and methods, 'know-how' - underlying the detailed design, which is owned by the original designers, can be more challenging to acquire.

c) Accountabilities and roles of responsible designers

During the construction and commissioning of existing nuclear plants, various consortia models were used, which in some cases raised questions about where responsibilities lay at a particular time. When exactly should the utility assume its Design Authority role? Moreover, depending on its size or organizational structure, the utility may not be able to acquire by itself all the detailed, specialist design knowledge of all the systems and components important to safety. For plants sold on a turnkey basis, it is even more challenging for the operating company to obtain and maintain all the knowledge needed for its Design Authority role. These issues are likely to become more challenging as the number of countries and utilities operating plants increases.

INSAG-19 recognizes that the accessibility of design knowledge is not a trivial matter, not least because the amount of information is huge: *"The operating organization must assure itself that a formal and rigorous design change process exists so 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 and added to throughout the lifetime of the plant"*.

It is specified in IAEA SSR-2/1 (requirement 3) that *"tasks that are assigned to external organizations (referred to as responsible designers)*

for the design of specific parts of the plant shall be taken into account in the arrangements". This provision is related to the fact that the operator may assign tasks for some parts of the plant to other entities that have the requisite design knowledge[2]. INSAG 19 states that *"the role and accountabilities of the 'Design Authority' within the operating organization, the specific roles that have been assigned to the responsible designers, the precise areas that the responsible designers are held accountable for, and the processes that must be followed for each of the parties to exercise their responsibilities properly, must be defined very clearly."*

Despite this guidance, there is no internationally agreed mechanism in place which would require the original designer to provide the detailed knowledge needed to fulfil the Design Authority role. Neither is there a mechanism to ensure that design knowledge is universally applied throughout the international fleet for the benefit of safety. The exploration of these topics, including the distribution of accountability between the licensee's Design Authority, which bears the prime responsibility for safety, and the "responsible designers", within a standardized fleet, forms the basis of the discussion in this paper.

[2] As stipulated in IAEA SSR-2/1 & INSAG 19: The Design Authority may assign tasks "to other entities that do have that specialized knowledge of detailed design; for the reactor system and its supporting systems this would likely be the original vendor of the system". According to IAEA SSR-2/1, the concept of "responsible designers" can include, beside the original "nuclear vendor" of the NSSS (Nuclear Steam Supply System), and as needed, other equipment suppliers (detailed designers for NSSS equipment as well as non NSSS suppliers).

2 CORDEL and Design Change Management

The World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group aims to promote standardization of nuclear reactor designs.

Standardization offers a unique opportunity to make optimal use of best practice and operating feedback sharing mechanisms and to maximize their contribution to nuclear safety.

Operating experience and measures for improving safety are being shared extensively amongst utilities, for example under the auspices of the World Association of Nuclear Operators (WANO). CORDEL has concluded that the industry should take the opportunity presented by standardization and strive to improve these mechanisms still further. This raises important questions: How can operating experience sharing be enhanced and the benefit of international standardization be maintained throughout a plant's lifetime when several reactors of the same design will be run by different operators in different parts of the world? How should the roles and accountability for design changes be allocated between utilities, vendors and responsible designers?

To address these challenges, in 2010 CORDEL set up the Design Change Management (DCM) Task Force, with the aim of sharing and analysing existing practices, to identify best practices, and to make recommendations to improve safety and maintain standardization throughout the lifetimes of the plants. Representatives from utilities, vendors, owners groups, WANO and the aerospace industry are members of this task force.

The DCM Task Force has analysed design change management within fleets of similar design stretching across a number of countries with different regulatory systems. This report examines a number of options to implement a Design Authority by reviewing some 'best-in-class' implementations by licensees, considering 'shared accountabilities' and reviewing support functions offered by owners' groups. The causes of design change and the reasons why design changes are not always systematically deployed in today's fleets are discussed. The report then considers the roles played in the design change process by plant utilities, vendors, regulators, owners' groups and other organizations such as WANO.

It should be noted that there are several options for utilities to organize themselves – including within owners' groups – to fulfil their responsibility as regards design knowledge and design change management. For instance:

i. a utility can have its own in-house engineering resources. This can be the case for big utilities (or a group of utilities) which have several units in operation. This company can also act as 'reference operator' through a dedicated relationship with smaller or isolated companies operating the same design;
ii. a group of utilities operating the same design can decide to incorporate and share their own engineering resources and experience feedback to acquire and maintain this design knowledge;
iii. utilities operating the same design can decide to group together and organize their work in closer connection with the original vendor and designers and to benefit from their involvement to establish design knowledge and share experience, with adequate contractual agreements.

This report by WNA CORDEL Working Group, which gathers both utility and vendor representatives' opinions, focuses mainly (though not exclusively) on this third option.

The fundamental issue for this review is to examine what design knowledge and design analysis capability must be retained over the lifetime of a nuclear plant (or fleet of units) by the plant owners/operators and vendor to make safe decisions for design and operating changes, under the oversight of the regulators.

3 Design Change and Lessons Learned from Fukushima

The March 2011 accident at Japan's Fukushima Daiichi nuclear plant raises a number of questions in the area of design change management. While the magnitude of the external hazard was clearly not taken into account in the original design basis, and the subsequent modifications of the original units, the accident highlighted fleet differences such as the containment hardened vent. This plant feature was required in the US and design specifications were developed under an owners' group initiative. However, detailed design and subsequent implementation varied, partly due to differences in the original plant design but also due to preferences of the individual operators. It provides a good case study for improving a fleet design change management process for the existing and for the next generation of plants, within a standardized fleet.

An operating organization is expected to encompass the role of the Design Authority for its plant. One interpretation would imply that every utility around the world should maintain all the design staff needed to understand in detail all the mathematical modelling of the safety case and of the behaviour of all the components of the plant, in order to understand all the consequences of a design change. Some of these design changes can be subtle. Some consider this an impractical (and also expensive) expectation, depending on the size of the utility. Operating organizations must, of course, maintain a sound knowledge and understanding of the plant and its safety case to be able to operate the plant safely, and to maintain it to designers' specifications. Only the largest utilities, however, can afford to retain by themselves a large design support staff throughout the life of the plant. So utilities can choose the path of making agreements with the vendor and responsible designers to fulfil their Design Authority responsibility. But even the largest utilities may not be able to come up with best technical solution for design changes in the absence of an international framework supporting exchange and compliance with best practice.

Sharing experience and benchmarking within owners' groups on what level of knowledge of the design should be retained by an operator (through its Design Authority) in order to ensure safe operation, maintenance and modification of the plant would be beneficial and could result in developing common principles. Alongside this, the knowledge of the designer should be maintained and used as an intrinsic element of design change management to ensure the continuing safety of the plant.

The objective that the operator by itself is wholly responsible for the design once a plant is in service is challenging to achieve today, and, with an expansion of the nuclear industry worldwide bringing with the potential for fleets of standard Generation III plants ordered on a turnkey basis, it could be even more challenging in the future. This raises the need to consider the principles and arrangements of a specific organization while drawing the benefits of a standardized fleet. This might also drive the way a turnkey contract is established, which must allow the operator to become a 'knowledgeable customer', able to take on board the 'ownership' of the design and to have a clear view of the importance to safety of design issues, in order to be able to take informed decisions regarding safety.

4 The Licensee's (Utility / Operating organization) Role and Responsibility

International standards make clear the primacy of the licensee's role in nuclear safety: "The licensee retains the prime responsibility for safety throughout the lifetime of facilities and activities, and this responsibility cannot be delegated. Other groups, such as designers, manufacturers and constructors, employers, contractors, and consignors and carriers, also have legal, professional or functional responsibilities with regard to safety" (IAEA-Safety Fundamentals-SF-1).

This responsibility can be broken into a number of areas, notably: establishing and maintaining the necessary competence; providing adequate training and information; establishing procedures and arrangements to maintain safety under all conditions; verifying the appropriate design and adequate quality of facilities and activities and of their associated equipment (cf. IAEA-SF1).

As already specified in the Introduction, according to IAEA SSR-2/1 –(Safety of Nuclear Power plants: Design) - req. 3, each operating organization *"shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant". It shall include "a formally designated entity responsible for the safety of the plant design within the operating organization's management system, and tasks that are assigned to external organizations (referred to as "responsible designers") for the design of specific parts of the plant shall be taken into account in the arrangements."*

There are a variety of situations to consider. These include relatively small utilities operating a small number of units in a rather isolated context, utilities operating similar units in the same country and facing the same regulator, through to large utilities operating large fleets in different countries, and there will be combinations of these.

For small utilities, it may be challenging to have adequate engineering resources to know by themselves, in sufficient detail, the design they operate and all the reasons behind the design choices made by the vendor and the responsible designers. However they should have developed sufficient knowledge of the design to be a 'knowledgeable customer' and to know what is important to operate their plant safely. This is where the relationship between the utility and the original vendor becomes important in order to take advantage of the vendor's own 'Design Authority' capability; this would require long-term agreements with commercial implications.

When several utilities are operating similar units in one country (as is the case in Japan, Germany and the US), they work with the same regulator, and it is beneficial for them to define common positions on safety issues. VGB in Germany and NEI and owners' groups in the US are organizations that play this role of bringing the utilities together to develop a common solution to the same safety/regulatory issue, which in itself contributes to keeping the units similar. In the context of new build, several US utilities have applied for combined Construction and Operating Licenses (COL) to build the same few designs. The NEI New Plant Working Group was set up in order to facilitate and speed up the licensing process, which in itself supports standardization. Having achieved standardization at the licensing stage, utilities should be encouraged to continue this kind of cooperation during the life of their plants and this is also a potential role for owners' groups (Candu owners' group plays this role for some common issues – see Section 6).

For utilities operating a number of similar units in different countries

through subsidiaries, they have significant incentives to keep similarities between these units which include sharing operating experience, sharing spare parts and the benefit of a common engineering team serving the whole fleet. Even if the subsidiaries are different companies operating in different regulatory environments, it is likely that these incentives will prevail.

It is important in all situations that the relationship between a utility and its vendor is maintained after plant start-up. Some form of contractual agreement or cooperation should be put in place on a long-term basis to ensure the knowledge management of the design as needed. Utilities may struggle to fully understand the design basis before making any change to their plants, but ultimately, they are the only ones legally responsible for the decision.

The concept of a utility's Design Authority should be implemented, while recognizing the importance of the original designer in design knowledge and design change management, as was pointed out by INSAG-19.

Utilities should recognize the benefit of participation in owners' groups, and should play an active role in their organization for standardized units by sharing enhanced experience feedback. They should also make maximum use of cooperation with their international peers within international organizations such as WANO.

5 The Importance of the Vendor and Responsible Designer's Role

As explained in footnote 2, the concept of 'responsible designers' (IAEA SSR-2/1) can encompass, beside the original nuclear vendor of the NSSS (Nuclear Steam Supply System), other equipment suppliers (detailed designers for NSSS equipment as well as non-NSSS suppliers). Their role also has to be considered by the utilities for example within their owners' group. Often it is they who retain the detailed knowledge of why the design is how it is. Responsible designers, therefore, need to be involved to a great extent in keeping and improving the safety of a design during operation.

The vendor should also play an important role in remaining up to date with new research findings and developments, particularly as impact the understanding of the design basis for the plant, and with changes in the design of the plant.

In general, the distribution of responsibility[3] for design change management varies according to the safety classification of a system, structure, or component (SSC). When the plant is first built and during its early years of operation, the original NSSS designer has a large degree of responsibility for any design changes of safety-related SSCs. This was the case with the first and second generation of nuclear plants.

As designs and the regulatory requirements evolved, the relative distribution of these SSC classifications changed. A larger proportion of plant systems and components are now considered important to safety (Figure 1).

As a licensee's fleet size increases, however, the 'cost' (engineering workload) of 'owning' the design basis for standardized designs, even for safety-related SSCs, decreases, as the cost is spread across many units (Figure 2).

For a small utility, with a small number of plants, the increased burden driven by the increase in the number of SSCs considered to have safety attributes may require more support from the original designer.

Figure 2 illustrates historical precedence for a licensee's "ownership" of the design basis. This might also be applicable in the future if a licensee (or country) were to build a sufficiently large fleet of a standard design. India, for example, has plans for building multiple units of imported standard design. In such a case, the licensee may have the desire and capability to own more of the design basis than a country or utility with only one plant of that design. Either way, the vendor needs to share in ownership of the design basis with the licensee's Design Authority, this sharing of ownership being tailored to the licensee's capability.

Each operating organization has the responsibility to collect and analyse the experience feedback (beside international experience feedback for major issues). This operating experience may be shared with other utilities within the owners' group in order to improve both the safety and performance of standardized units. It can also be shared, or partly shared, with the vendor/responsible designers which could be assigned dedicated tasks in connection with their detailed design knowledge. Reciprocally, the vendor would also keep utilities informed and draw their attention to any emerging issues related to design and to maintaining the design basis document.

For standardized reactor designs the role of the vendor/responsible designers in fleet oversight

[3] Responsibility here refers to technical knowledge and contractual responsibility. Prime responsibility always lies with the licensee.

internationally is even more important. Vendors, in close collaboration with utilities as knowledgeable customers, can play an important role in the exchange of information and operational experience within 'their' fleets across the world. They can help maintain design knowledge and play an enhanced role, in interaction with utilities/licensees, in studying and proposing design improvements which might result from this experience feedback.

For example, the role of the vendor / responsible designer, which could be shared with the owners having the whole operating experience, could include analysis of operating experience related to failure modes and failure rates of similar components in a fleet. This could result in the dissemination of operating experience that has implications for design and potential design changes through a strengthened 'service and advisory bulletin' system. The compiled data could be far more detailed and valuable than of today as this 'cost' is spread over the whole fleet. Currently, every utility's responsibility would be to maintain such a database, by itself or through arrangements with responsible designers.

The use of 'service and advisory bulletins' on both safety and operational matters needs strengthening and should include a graded approach reflecting their safety significance. The most important matters should be assessed by utilities in order to decide what action (if any) should be taken: implementation or adaptation, taking into account local context or regulatory framework. Utilities should provide feedback to the designer regarding actions taken to address the bulletins.

Most vendors have developed or are developing inside their organization what some vendors call their own 'design authority', consisting of a group of engineers who maintain a historical record of the various designs they have produced and all the reasons behind the design choices. Their role is to review any changes proposed to or by their customers to check compatibility with the original design intent. This kind of organization is important for ensuring the success of the modifications considered (be it for performance or safety improvements).

However, the final decision (modification, improvement,

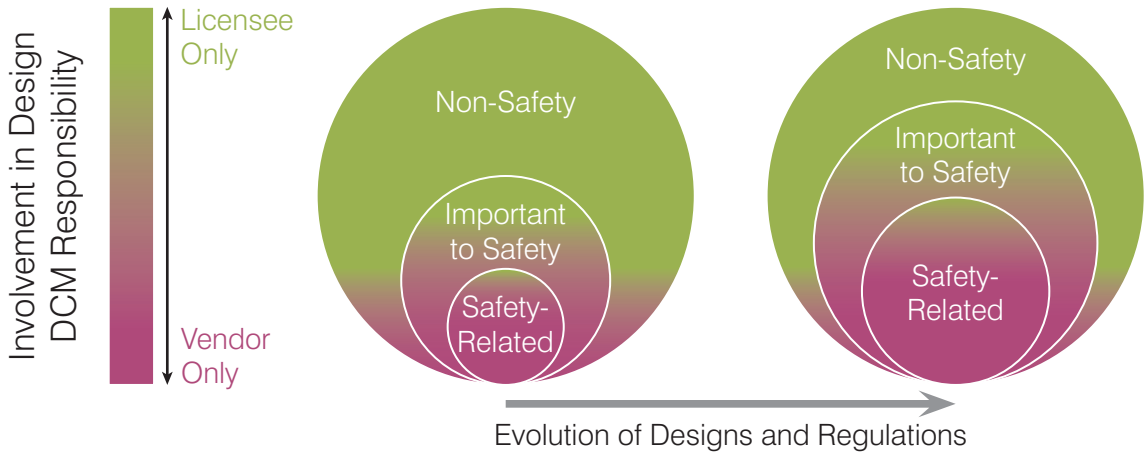

Figure 1. Increasing number of safety significant SSCs with the evolution of regulation entails increasing contractual responsibility for the vendor

experience feedback *etc*.) lies with the licensee (utility), taking into consideration its own local context.

In the case of the vendor's business being transformed, changing ownership or ceasing to exist, it is important to ensure that the vendor's IP (Intellectual Property) assets (including its human resources) are maintained and transferred to another technically competent organization. This role might be assumed by a relevant owners' group.

This emphasizes the need for a well-established knowledge management system as knowledge will have to be passed across successive generations of engineers within vendors, responsible designers but also within a licensee's Design Authority.

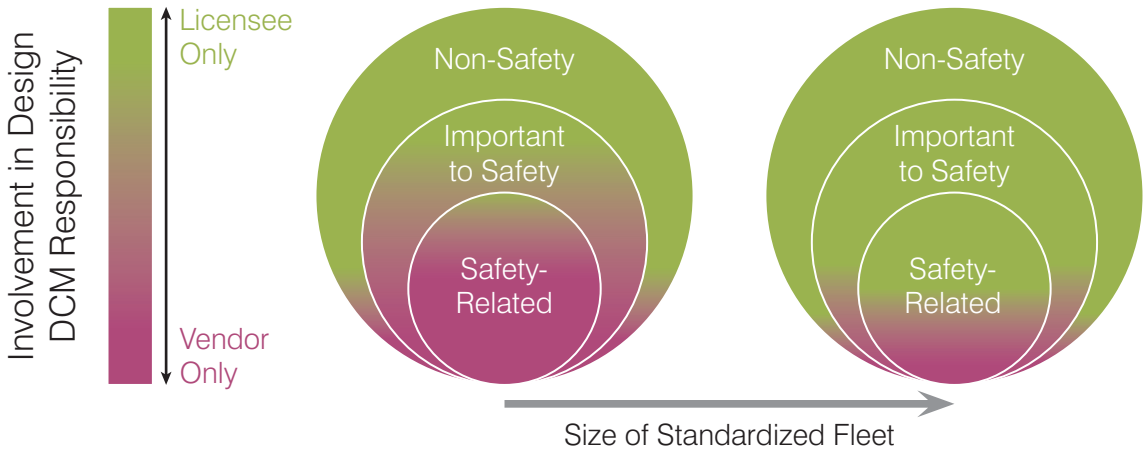

Figure 2. Increasing licensee's ownership of design basis with the increase of licensee's standardized fleet size entails less contractual responsibility for the vendor

6 The Owners' Group Role for a Standardized Reactor Fleet

Owners' Groups (OGs) are organizations that bring together utilities operating nuclear plants of similar technology. They also generally include the original vendor of the corresponding technology. The owners group provides a convenient forum in which the utilities that operate the vendor's design, and the vendor (and with possible other responsible designers for main components) can share operating experience and common technical issues and the ways to solve them[4].

A survey of OGs has been carried out by CORDEL involving:

- AREVA Owners' Group (still known as Framatome Owners' Group or FROG).
- OKB Gidropress (Russian NSSS designer).
- CANDU Owners' Group (COG).
- PWR Owners' Group (PWROG, formerly the Westinghouse owners' group).
- Japan PWR Owners' Group (for MHI-designed plants).
- Boiling Water Reactor Owners' Group (BWROG, GE-Hitachi's design).

These OGs operate in a variety of circumstances: some are single nation groups with a single common regulator; some include utilities operating in different countries with different regulators; some also cover the situation of a single utility linking back to the vendor's 'reference' country. These circumstantial differences could account for many operational differences.

Usually OG membership is voluntary and assigns no responsibility to the vendor for recommending standard solutions or for influencing utilities to implement them.

Some strengths and good/best OG practices can be identified from the survey.

Findings of the survey are as follows:

- **Participants:** all OGs include the vendor(s) and utilities operating this vendor's reactors.
- **Voluntary or mandatory utility involvement:** involvement is voluntary except in Russia, where the national regulator mandates involvement with the original designer. In some cases, utilities are motivated to join by the membership benefits offered. There is no mandatory requirement for membership at the international level, with the exception, perhaps, of the VVER operators in Ukraine, where the national regulator demands mandatory adherence to the the original designer's safety recommendations.
- **OG charter:** most OGs have a relatively detailed charter which the member utilities sign up to. In some cases, only utilities – and not the vendor - are voting members (AREVA Owners' Group, and currently under review for COG).
- **Primary areas of activity:** OG activities include sharing operational experience, reviewing common safety, reliability, and regulatory issues and even plant economics. In some cases, issues might be addressed through shared research and development. OGs have the flexibility to share operational experience: the sharing mechanisms can be arranged around design-specific features or around a secondary supplier's issue who may only participate in the relevant activity. The participation may be voluntary, for example where cost sharing is involved.
- **Database of licensing and safety issues:** although the survey results showed that not all OGs keep a database of design-specific issues, there is usually an alternative, for example: a website listing common issues and analysis (most OGs); the

[4] IP ownership can be a potential barrier to sharing information on design and may require adequate contractual provisions between the OG members to be in place.

[5] While not strictly related to the scope of this document, the OGs could be a forum for sharing and exchanging about methods used to take into account external events which could have an impact on the design.

[6] In this process, risk assessments of regulatory compliance issues are evaluated by NRC staff using generic PRA models maintained by the NRC. These models are continuously improved through interactions with licensees who maintain detailed, plant-specific PRA models.

provision of advisory bulletins (COG); or vendor's support delivered via televised conferences from vendor's crisis centre (Gidropress).

- **OG accountability for plant design and analysis:** generally the OGs, as expected, do not accept any accountability.
- **OG accountability for plant configuration management:** again, OGs do not generally accept accountability. However, there were some exceptions to this: in Russia and Ukraine, the vendor's agreement to any design or configuration change to the design basis is mandated by the regulator.
- **OG accountability for plant design changes:** Generally none accepted.

Several conclusions can be drawn from this overview of OGs' operations:

- It would be worth considering the introduction in the OG mandates of an objective to maintain the benefit of standardization, so if a design issue were to be identified by a member of an OG, all members should consider the issue's resolution and its implementation. In this context, developing a consistent approach to safety reassessment or Periodic Safety Reviews (as required), which would include international experience feedback and new knowledge, would be an important goal. The vendor analysis and proposals in relation to safety improvements can be beneficial.
- OGs should define a process to ensure that the knowledge of the main design differences between plants in the fleet is maintained and accounted for. This should involve the vendor.
- Using cost/benefit analysis, a utility can make informed decisions about whether or not it should carry out modifications or implement other measures. Probabilistic Risk Assessments (PRAs) are a basic element in this analysis, and can be used both for internal and external events[5] that can lead to common cause failures (depending upon siting and layout). For major internal events, similar plants should have similar risk profiles, provided that the data input into the PRA comes from a valid common database. OGs could develop standard PRA techniques related to their relevant designs for main internal events and collect reliability data from utilities operating these designs as input to PRA (subject to contractual arrangements or statute linked to use of proprietary information or IP). The shared benefits of a modification related to such internal events could then be demonstrated to all utilities within the OG, with the support of the vendor. This would help to avoid implementation of different technical solutions, thus maintaining standardization. This concept has already been demonstrated by the US NRC Reactor Oversight Program[6].
- Given the longevity of a nuclear plant, one of the most important issues is how the design knowledge should be maintained if the original designer is no longer available (for example, if it is no longer in business). The preferable solution is that the designer's IP is taken over by a new design organization. There may be several such changes over an operating lifetime spanning several decades. The duties, competence and responsibilities of replacement design organizations must be well defined and understood at the time of takeover. However, if no new design organization is available to take over the responsibilities and assets of the designer, the OG could take on this role for the whole fleet as a last resort.

For the benefit of safety and standardization of plants during their lifetime, there would be value in developing a consistent approach to safety reassessment (or Periodic Safety Reviews as required), which included international experience feedback. A vendor's analyses and proposals in relation to safety improvements could be beneficial. These reassessments, in turn, may produce new relevant safety-related recommendations, which can be shared between the vendor and other utilities through OGs or other operating experience exchange mechanisms, such as WANO.

In general, all relevant safety-related data should be benchmarked between the licensees within the OG to inform decision-making. For the most important issues, there should be a clear decision process by the licensee, based on a graded approach in relation to safety importance. Of course, in parallel, the regulatory bodies will also exert their independent scrutiny and assessment and share their views.

This system would demonstrate the safety and economic benefits of maintaining standardization (which does not necessarily mean full identity). There can be some agreed commitment or charter related to this principle within the OG. But it is clear (and it is the current industry experience) that there are other factors which are also in the licensee's consideration (such as local context) that could result in another decision framework.

7 WANO role

The World Association of Nuclear Operators (WANO) is a well-established and recognized organization of worldwide nuclear operators. With its operating experience program and the peer review program, WANO provides a unique tool for improving performance and safety of operating plants. Currently, the SOERs (Safety Operating Experience Reports) and SERs (Significant Event Reports) that are widely distributed among its members are extensively used by operators.

Considering design aspects, the Fukushima event has led the nuclear industry to question whether WANO activities have been too narrowly defined around operational excellence, without taking into account enough consideration of design features. In response, the WANO Design Project has been established to provide recommendations for expanding the scope of WANO activities to include some aspects of design.

The WANO approach is based on the following assumptions:

- Nuclear safety of a plant depends both on its design basis and operational performance.
- Criticality of systems or transients, and safety consequences of observed facts during peer reviews strongly depend on design characteristics as well as operational performance.
- Design understanding and management is one of the factors in major damaging events.
- Design is a living object which has to be reviewed in order to be up-to-date, taking into account events or new findings, naturally while keeping control of the safety margins.

In order to take into account all these elements, WANO is currently improving the way in which design insights are applied in the peer review process in order to:

- Focus attention of the peer review on the aspects of the plant's operations having the highest safety impact.
- Link and weigh the performance of the operating organization (peer review findings or Area For Improvements) against fundamental design aspects.

It is possible for non-regulatory organizations which are not operators, such as vendors or responsible designers, under contractual arrangements with WANO to have access to some information restricted to WANO membership. As this report advocates a better cross-involvement of utilities and responsible designers or original vendors regarding standardized units, CORDEL strongly recommends that – within the WANO framework - operators be encouraged to find an efficient way of sharing information within their OGs and that through such an exchange the vendor/ responsible designers could make use of experience feedback and analysis made by utilities (knowledge, lessons learned *etc*.) and propose a common solution to its customers in the most efficient way. Better usage of OG platforms should be investigated in that respect.

8 Regulator Role

Regulators are making efforts to harmonize their activities and share assessments of new designs. The Multinational Design Evaluation Programme (MDEP) is the best known initiative in this direction. It might be expected that the results of this work will not only benefit the initial standardization of designs during licensing, but also will support the benefit of standardized solutions during plant lifetime.

One concept that has been discussed, potentially as a long-term end state for MDEP, is the formation of 'Regulators' Groups' in which a number of regulators meet periodically and share operating and regulatory experiences with a common design. Such sharing of analysis and resources between regulators can also be a beneficial outcome of standardization regarding safety.

Examples of such regulatory groups exist, namely: the CANDU Senior Regulators' Group and the VVER Regulators' Forum. Alignment of the charters of Regulators' Groups and of the OGs could ensure timely and cost-effective implementation of regulator-requirements related to design changes with additional assurance of a consistent design across multiple regulatory frameworks.

This is already the case with the 'EPR Owner-Operators' Group' (established by EDF, in connection with the original NSSS designer AREVA) which interacts regularly with the EPR Working Group (EPRWG) of MDEP. This OG works on harmonized solutions to generic issues, and keeps track, with the support of AREVA, of the differences between the EPR projects and together with the regulators within EPRWG addresses the causes of these differences and works on maintaining harmonisation.

Given that progress in making reforms is likely to be slow, there are some actions that could be undertaken now which could help maintain consistency between similar plants under different regulatory influences. Two committees of the Nuclear Energy Agency (NEA) of the OECD, the Committee on the Safety of Nuclear Installations (CSNI) and the Committee of Nuclear Regulatory Activities (CNRA) that includes a large number of countries from OECD membership, have been taking initiatives to develop a common analysis process for some important generic plant events between regulators and their Technical Support Organizations (TSO). Task forces and workshops have been initiated on, for example, the sump clogging issue (identified in Barsebäck, 1992) or the electrical event at Forsmark (2006). These helped regulators to gain a better understanding of the event, lessons learned from the event as well as to come to consistent regulatory positions. These initiatives should be supported by the industry by providing the required technical inputs in this process. Industry (both vendors and utilities) should be encouraged to participate in these initiatives in a systematic manner.

Most utilities are planning for long term operation (licence extension) of their operating plants. Some regulators, especially in Europe, are using this opportunity to issue new safety requirements that could result in design modifications and further differences in similar plants. This process should be balanced as far as possible with respect to standardization efforts and the corresponding operational feedback sharing process. The nuclear industry clearly must be positive about safety improvements in the context of lifetime extension, but these should be reasonably practicable and applied across the industry in a harmonized way. The regulatory authorities should work with each other on this issue and both OECD/NEA and IAEA should play an instigative role.

9 Design Authority

The topic of Design Authority is fundamental to design responsibility, which includes the themes of this report: design knowledge and design change management. The principle of the operator owning the ultimate responsibility for the design of the plant implies that the operator is the 'authority', the decision maker. However, the other connotation of the word, implying expert or knowledge holder, refers to a vital capability which may be challenging for an operator to fulfil by itself in all details.

The original vendor of the plant may be in a good position to fulfil this latter capability, through suitable commercial arrangements to incentivize this.

There are examples of the original vendor no longer existing as a commercial entity which complicates this issue further and in such a case a solution would have to be found by the utilities within the owners' group.

A survey has been carried out by CORDEL to understand how different operators are approaching the subject of Design Authority. This covered five countries: Republic of Korea, Canada, USA, UK and France (EDF). The key questions asked were:

- How is design knowledge acquired and maintained over the life of the plant?
- How is the Design Authority role executed?
- What is the role of the original designer?
- How does the Design Authority discharge its responsibilities for design change and configuration management?
- How does the Design Authority ensure consistency throughout the fleet?
- How many full-time equivalent staff are in the Design Authority organization?

The results are summarized as follows:

- **In Korea**, the Design Authority for existing plants as well as for new build plants is a formally designated entity, called the Central Research Institute, which lies within the operator's (KHNP's) organization. KHNP has continuous access to the responsible designers, *i.e.* the original plant vendor KEPCO E&C and the component supplier Doosan. KHNP delegates detailed areas of the overall Design Authority responsibility to the responsible designers. Repeat projects are increasing the KHNP in-house Design Authority capability. KHNP and KEPCO E&C are both subsidiaries of the government-owned parent company KEPCO, which simplifies matters. Through OG membership, KHNP also gets support from overseas vendors for its CANDU and Westinghouse designs. Responsible designers take some Design Authority responsibility during construction and handover, and during the warranty period of two years (four years for the UAE project) of operation. During the plant lifetime, the Design Authority is maintained by KHNP with support from designers on a project-by-project basis and according to specific contractual agreements. For the UAE project, KEPCO is developing a 'Book of Knowledge' which would contain the knowledge base for the execution of the Design Authority function by ENEC. This model, of operator and designer being part of one company, of obligating the vendor/original designer to have roles in the Design Authority, and of the increasing Design Authority capability through succession of standard projects, is deemed to be a good model and merits further study.
- **In France**, EDF is the operator and architect-engineer of its plants (EDF does not enter into turnkey contracts). EDF has an internal organization called Nuclear Engineering Division (DIN) whose role, among others, is the design organization (according to SSR-2/1) and the Design Authority (according

to INSAG 19). DIN is a senior-level division which also coordinates the allocation of design-related activities among various EDF engineering centres. A contractual relationship with the original NSSS vendor (Areva) is maintained, but EDF has developed its own deep design knowledge. EDF always seeks to incorporate international experience feedback during Periodic Safety Reviews, and some urgent actions are implemented without having to wait for PSRs. This model works very well through consistent operation over a long-term programme. Whilst a very good practice, it may be challenging for other utilities to achieve a capability the size of EDF's, which has been built up over a long period. But there are lessons to learn, particularly in the consistency of EDF's fleet-wide approach to design change.

- **In the USA**, reliance on the original designers (NSSS vendors) is recognized, as they are the IP owners. Also, Original Equipment Manufacturers (OEMs) and OGs sometimes develop design modifications and these have resulted in design changes in older plants being implemented in different ways according to the licensee's decisions. In future, a more clearly defined joint ownership of design basis between the operator and designer should be possible, potentially based on Probabilistic Risk Assessment.
- **In the UK**, the original plant designers no longer exist as separate legal entities for some of the plants although processes have been in place for knowledge transfer to the current organizations. The role of Design Authority is invested in an individual, supported by a team whose aim is to have a full technical understanding of the plant. There is some evidence of difficulties in certain Design Authority areas. In such areas, delegation via clear contractual agreements with responsible designers is undertaken.
- **In Canada**, the Design Authority is the Chief Nuclear Engineer within the licensee's organization. He may formally delegate some aspects of Design Authority to plant engineering staff and to a 'design agency' but not overall accountability. Requirements for this process and role are captured formally in Regulatory Document RD-337 *Design of New Nuclear Power Plants* (based on IAEA SSR-2/1), and in the licence itself. For new build in Canada, the roles of vendor and operator, and the transition of Design Authority from vendor to licensee during handover, are being clarified.

It is clear that there are many common experiences in different organizations but there are also many subtle differences due to, not least, different maturity levels and situations. The right balance regarding design knowledge ownership between corporate and plant level is also a subject relevant to each utility responsibility.

Further work is required by CORDEL to extract all the learning and to define functional aspects or principles for a Design Authority within operating organizations, in connection with WANO. This work would address key issues around the need for the Design Authority within operating companies to have a strong link with an owners' group, and also with the vendor (and responsible designers) through commercial operator-vendor relations.

Of course, the regulatory bodies will keep their oversight on this important issue.

10 The Aerospace Industry Model

In addition to the ideas developed in the CORDEL 'roadmap' report [6], discussions have been held with representatives of the aerospace industry on the basisthat they also operate in a highly technological industry in which reliability and safety are vital. The experience feedback from aerospace industry's internationally regulated certification process for standardized types of plane holds some interest for the nuclear industry[7].

Techniques for adhering to standard designs at an international level were developed many years ago. There are several lessons to be learned, which are covered by a separate report [7], including:

- Achievement of a UN-backed political agreement on the acceptance of basic safety requirements and rules (Chicago Convention Annex VIII).
- Creation of a pan-European type certification agency (European Aviation Safety Agency, EASA).
- Detailed understanding of the Type Certificate process and bi- and multilateral acceptance agreements.
- Design change management and maintenance of Type Certificate throughout design lifetime (through use of Airworthiness Directives and Service Bulletins).
- Interfaces of responsibilities and allocation of risks and liabilities among designers, manufacturers and operators.
- Execution of Design Authority role by manufacturers.
- Industry joint processes of standards development and manufacturer's certification.
- Responsibility of national regulators within an internationally agreed framework.

[7] CORDEL equally recognizes that the context is different: for instance, the international nuclear liability regime channels responsibility exclusively to the nuclear operator.

11 Conclusions and Recommendations

For a long time, standardization was mainly seen as a tool to improve nuclear plant economics during design approval, licensing and construction. But successful examples in several countries have demonstrated that standardization can also bring significant benefits to plant safety during operation as it offers a wide international basis for experience exchange from the entire fleet of standard plants worldwide. In order to retain the benefit of standardization throughout plant operation, an international fleet-wide approach to design change management has to be seen as a vital concept.

WNA's CORDEL Group has been investigating existing and new mechanisms which might deliver improved benefit from design standardization throughout a fleet's lifetime. CORDEL's main focus has been on new-build plants where the opportunity for standardization is greatest, but some of these recommendations are also applicable to existing fleets.

The Fukushima accident provides an example of institutional problems in the management of nuclear power plants' operation and the lack of an international mechanism that encourages design changes to be implemented across a fleet of similar plants, especially regarding severe hazards.

The likely global expansion of nuclear power, together with global sales of a small number of turnkey new-build designs will result in fleets spanning a number of utilities and countries. For some utilities, particularly smaller ones where there are limited engineering resources, it may be challenging to fulfil their Design Authority role up to a detailed level.

IAEA SSR-2/1 and INSAG-19 recommend the utility's accountability for nuclear safety, and therefore for plant design definition, through a formally designated entity responsible for the safety of the plant design within the operating organization (Design Authority). However, further work needs to be pursued to identify best practices with respect to discharging the Design Authority function. Therefore the ability of utilities to meet this accountability in all circumstances and all level of details could be challenging. Support from or reliance on the plant vendor and responsible designers will be beneficial in many situations through a sustainable business model based on clear contractual responsibilities.

The existing mechanism of the owners' group (OG) already provides a good point of interaction between the utilities and the vendor / responsible designers. And although OGs are mainly based on voluntary utility involvement, they hold the potential for further cooperation in design standardization. WNA CORDEL can only strongly support and encourage membership of all utilities operating the same design in OGs, on a worldwide basis, even if different regulatory regimes bring some limitations in the globalisation of solutions that are implemented. In particular, operators could benefit from sharing with vendors relevant elements of experience feedback and related analysis at the fleet level when design issues are involved.

There is also successful experience of Regulators' Groups in which regulators working on a common design of plant meet to share experiences, seek to harmonize their activities, and target a common approach (MDEP design specific WG).

Discussions with the aviation industry have identified some key areas of potential common interest.

CORDEL makes the following recommendations to address issues raised in the above conclusions and to pursue the benefits of design standardization in general:

Design Change Management and Design Authority

There is a need to develop an international industry framework that:

- Clearly defines the respective roles and responsibilities of the utility and vendor in the international design change management process.
- Describes how the utility defines its relationship with the vendor with the view to fulfilling its Design Authority role.

Owners' groups are in a good and privileged position to provide a forum in which utilities can share knowledge and assessment of generic safety-significant issues and potential generic design changes with the support of the vendor, and bringing in other utilities' contributions where needed. This vendor's role should be clearly defined in vendor-utility agreements which should include initial design information handover and the potential for changed circumstances of the parties throughout the lifetime of the plant.

The focus of these agreements should be to maintain design standardization in all design change decisions, with best practice being shared internationally across the fleets.

Further work is required by CORDEL to extract the learning, and propose the functional aspects or principles for a Design Authority implementation within operating organizations in connection with WANO. This should include a definition of Design Authority that can be applicable to many different utility/vendor/regulator scenarios. It should cover how the role of the Design Authority, which rests with the operator, can be enhanced and made to work across different organizations with different organizational structures, involving utilities and vendors/responsible designers, and commercial arrangements, and without resulting in an unnecessary cost burden.

Owners' Groups

More detailed work with OGs is recommended and should address:

- The possibility of increased opportunities by OGs for standardization through joint review and implementation of design changes, and by developing benchmarks where there is a need for alternative solutions, with a goal to maintain standardization.
- How to strengthen as appropriate the involvement of the original vendors in OGs, including the use of vendor service and advisory bulletins within the OGs.
- How to strengthen the role of the OGs with respect to identification and knowledge sharing of significant safety issues, which then should result in decisions by utilities to be benchmarked between all OG members.
- The sharing within OGs of reliability data for main internal events related to design and standard equipment to be included in PSAs.
- The production of OG best practices (including on sharing common principles on the functioning of Design Authorities).
- As far as practical, an efficient screening process related to prevention, performance monitoring, accident management and mitigation.

WANO

Further discussions with WANO about strengthening its role regarding design aspects are recommended. These should include:

- Developing WANO's relationship with OGs where OGs could help produce reports on design-specific issues for dissemination among participating utilities.
- The development of design-informed peer reviews which should help to identify safety issues or challenges to safety functions, especially within a standardized fleet.

Regulators

The benefits of design standardization to safety throughout operating lifetime should be recognized by regulators. Regulators might consider (consistent with MDEP):

- Setting up Regulators' Groups and task forces and conducting workshops for specific emergent technical problems.
- Developing common guidance on generic safety issues in order to bring consistent answers and improvements through modifications during Periodic Safety Reviews (PSRs) and lifetime extension processes. These could then better include international experience feedback. In turn, these PSRs themselves could also produce new relevant safety-related recommendations, and these could then be passed onto the utilities and vendor through OGs or other operating experience exchange mechanisms.

Other Industries

Further discussions with the aerospace industry should include:

- Regulatory harmonization and Design Authority management.
- Lessons learned from the Type Certificate process and the interfaces of responsibilities.

12 References

[1] 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

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

[3] Convention on Nuclear Safety, International Atomic Energy Agency, 1994

[4] IAEA Safety Standards, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1, International Atomic Energy Agency, 2012

[5] Benefits Gained through International Harmonization of Nuclear Safety Standards for Reactor Designs, World Nuclear Association Discussion Paper, January 2008, http://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/ps-cordel.pdf

[6] International Standardization of Reactor Designs, WNA CORDEL Working Group, January 2010, http://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/International%20%20Standardization%20of%20%20Nuclear%20Reactor%20Designs.pdf

[7] Aviation Licensing and Lifetime Management – What Can Nuclear Learn?, WNA CORDEL Working Group, January 2013, http://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/CORDELAviationReport.pdf

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 the standardization of nuclear reactor designs. This can only be achieved by the development of a worldwide regulatory environment where internationally-accepted standardized reactor designs, certified and approved by a recognized competent authority in the country of origin, can be widely deployed without major design changes due to national regulations.

This report entitled *Design Knowledge and Design Change Management in the Operation of Nuclear Fleets* looks at existing and new mechanisms which might deliver improved benefit from design standardization throughout a nuclear fleet's lifetime. Building upon the licensee's prime responsibility for any design change through its Design Authority, it examines the interactions with vendors and responsible designers, as well as with operating organizations, such as owners' groups and WANO.

The World Nuclear Association is the international private-sector organization supporting the people, technology, and enterprises that comprise the global nuclear energy industry. WNA members include the full range of enterprises involved in producing nuclear power – from uranium miners to equipment suppliers to generators of electricity. With a secretariat headquartered in London, the WNA serves as a global forum for industry experts and as an authoritative information resource on nuclear energy worldwide.