WNA Report

Design Change Management in Regulation of Nuclear Fleets

A Report by the World Nuclear Association's Working Group on Cooperation in Reactor Design Evaluation and Licensing (CORDEL Group)

World Nuclear Association

Contents

World Nuclear Association's Working Group on Cooperation in Reactor Design Evaluation and Licensing (CORDEL) promotes standardization of nuclear reactor designs on the merit of improved economics and safety offered through building reactors in series and capitalizing on the broad basis for experience exchange.

Summary

The 60-year life of a reactor means that a plant will undergo change during its life. To ensure continuing safety, changes must be made with a full understanding of the design intent. With this aim, regulators require that each operating organization should have a formally designated entity responsible for complete design knowledge in regard to plant safety. INSAG-19 calls such an entity the 'Design Authority'.

This requirement is difficult to achieve, especially as the number of countries and utilities operating plants increases. Some of these operating organizations will be new, and some will be small. For Generation III plants sold on a turnkey basis, it is even more challenging for the operating company to develop and retain the full knowledge of the design of the plant needed for this role.

CORDEL's Design Change Management Task Force is investigating options for effective design change management with the aim of supporting design standardization throughout a fleet's lifetime by means of enhanced international cooperation within industry and regulators.

This report starts with considering the causes of design change and identifies reasons for the increased beneficial involvement of the plant's original vendor in the design change process. A key central theme running through the report is the definition of responsibilities for design change. Various existing mechanisms of vendor-operator interfaces over design change and how they are managed in different organizational and regulatory environments around the world are considered, with the functionality of the Design Authority role and its impact on owners, designers, and Owners Groups being central. The roles played in the design change process by vendors, utilities, regulators, Owners Groups and other organizations such as WANO are considered. In addition, the aerospace industry approach to Design Authority has been assessed to consider what lessons might be learned.

1 Introduction

If the risks and uncertainties in the cost and time of building and licensing Generation III reactors around the world are not minimized, the world's reduction of its carbon footprint from electricity generation will be rendered more difficult to achieve.

International safety concerns, uncertainties in licensing, cost overruns during construction, and performance optimization during operation and eventual decommissioning can be addressed through standardization of design across international fleets, and through maintaining that standardization throughout the fleet's operating lifetime. Standardization that is maintained throughout that fleet's life can be expected to enhance the safety of the individual units of a worldwide fleet.

I a. Causes of design change

The 60-year life of a reactor means that a plant will undergo significant change during its life. INSAG-19 [1] clearly describes reasons for changes in plant design, such as: physical ageing of systems, structures and components; obsolescence that inevitably occurs in many of hardware and software elements; feedback from operating experience and from research on unexpected design issues; changing regulatory standards and best available techniques; and changes in performance and organizational structure.

A fundamental principle of the nuclear industry is based on the operator's prime responsibility for safety [2,3]; this involves the licensee's ultimate responsibility for the design and design changes. What influences the operator to consider design changes implemented by others will vary across the world but there is often little consideration for standardization in such circumstances. Design modifications, agreed to by most operators, could be rejected by others for economic reasons. Over time, originally standardized reactors will tend to become unique and the safety benefits of experience feedback could be impaired.

It is important to learn from the successful experience of currently operating standardized nuclear fleets in our own industry (e.g. French fleet, VVER fleet, etc.) and from other industries, such as the aerospace industry.

There is a benefit to safety in maintaining standardisation within a fleet. It is much easier to learn from the operating experience of similar plants. Further, Generation III plants are expected to achieve a much lower failure rate than the very low rate already achieved. It is important to ensure any barriers to learning from experience are minimised.

I b. Current legal situation in the nuclear safety regime

International discussion and agreement on standardized designs that achieve an acceptable level of reactor safety across many jurisdictions is under development but still has a long way to go. The licensing processes needed to maintain that standardization have barely been discussed.

The legal framework currently in existence in the nuclear industry holds the operating company solely responsible for the safety of design and operation. The operator is also the one liable for third party damages in case of an accident. The nature of nuclear power plant design and construction involves many players – architect-engineers, nuclear island and balance of plant designers – as well as the necessity to adapt the design to specific site conditions. All this creates a large, complex and quite often unique infrastructure project with the operator carrying overall risk and responsibility for safety.

Regulators currently expect that every licensee maintains a complete understanding and knowledge of the design of every licensed unit. The IAEA Safety Standard SSR-2/1 [4] calls for the licensee to maintain design integrity and knowledge within the licensee's own organization in an internal entity called the 'Design Authority'.

In comparison, in the aerospace industry, the designer carries the role of the Design Authority for its own part of the aircraft whilst the operator still retains responsibility for airworthiness, and there may be lessons to learn from this.

I c. Is there a problem?

In the construction and commissioning of Generation II nuclear plants, there were different consortia models with little clarity of ongoing responsibilities. The utility is expected to take on the role of Design Authority. However, it might not and, in many cases, probably does not retain all the detailed, specialist knowledge required of all the systems and components important to safety needed to execute this role.

The Fukushima accident provides us with an example in this respect. Design changes which could have mitigated the consequences of the accident may have been available but were not fully implemented.

For Generation III plants sold on a turnkey basis, it is even less clear that the operating company will have all the knowledge needed for its role. The challenge of maintaining the necessary level of detailed knowledge at every plant in the world is bound to become more difficult 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. Design changes, that are made to a plant without a complete knowledge of why the plant looks like it does, can be detrimental to safety.

There is a provision in the requirements, however, that enables the operator to assign its responsibilities for some parts of the plant to other entities that have that knowledge – to a so-called 'responsible designer'. The role and responsibilities of the responsible designer "must be very clearly and formally defined".

It is considered, however, that there is no internationally agreed mechanism in existence which would ensure the role of the original designer in providing for that detailed knowledge and for ensuring that this design knowledge is universally applied throughout the international fleet for the benefit of safety. The clear definition of the responsibilities and distribution of accountability among the licensee's Design Authority, responsible designers, regulators and international organizations is the subject of discussion in this paper.

2 CORDEL Working Group and Design Change Management

One of the World Nuclear Association's Working Groups, Cooperation in Reactor Design Evaluation and Licensing (CORDEL), addresses the issue of standardization of nuclear 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.

The 'roadmap' report recognizes that although there is already an existing mechanism to share operating experience under WANO (World Association of Nuclear Operators), several questions remain unanswered, e.g. how to ensure that lessons learned from this operation experience (OPEX) are uniformly addressed by operators worldwide so that international standardization throughout plant lifetime is maintained? How to allocate responsibility for design changes between utilities and vendors? And once we see several reactors of the same design in operation in different parts of the world and run by different operators, will the benefits of standardization be lost?

To investigate these issues, in 2010 CORDEL set up the Design Change Management (DCM) Task Force to share and analyze existing practice, to seek best practice, and to make recommendations to stakeholders for the benefit of improved safety and the lifetime standardization of reactor design. Representatives from vendors, Owners Groups, utilities, WANO and the aerospace industry are members of this Task Force.

In this report, the DCM Task Force investigates, with the aim of improving, design change management within fleets of similar designs which will have different controlling environments such as stretching across a number of countries with different regulatory systems. This report examines a number of options to implement Design Authority by reviewing some peer 'best-in-class' implementations by licensees, considering 'shared accountabilities' and reviewing support functions offered by reactor-type Owners Groups. The report considers causes of design change and the reasons why design changes are not always systematically deployed in today's fleets. It then considers the roles played in the design change process by plant vendors, utilities, regulators, owners' groups and other organizations such as WANO.

The fundamental issue for this review is to determine over the lifetime of a nuclear plant (or fleet of units) what information and design analysis capability must be retained by the plant owner/operator, vendor and regulator to make safe decisions for design and operating changes. CORDEL is planning to seek views not only from within WNA membership, but also from selected regulators and international organizations, such as WANO.

3 Design Change and Lessons from Fukushima

The March 2011 accident at Fukushima raises a number of questions in the area of design change management. While the event was clearly beyond the design basis and the subsequent modifications of the original plants, the sequence of events that played out highlighted the differences in fleet implementation of features such as the 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, in part because of the variability in the original plant designs 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 next generation of plants.

An operating organization is expected to be the Design Authority for its plant. A strict interpretation implies 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 will be subtle, as in the case of Fukushima. Some consider this an impractical (and also expensive) expectation. 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 a large design support staff throughout the life of the plant. But even the largest utilities, as the case with TEPCO, may not be able to come up with best technical solution in design changes in the absence of an international framework supporting exchange and compliance with best practice.

Clarity is needed on what level of knowledge of the design should be retained by an operator, what level of knowledge is needed by the regulator, and how the knowledge of the designer should be maintained and be used as an intrinsic element of design change management to ensure the continuing safety of the plant. The objective that the operator is wholly responsible for the design once a plant is in service is very difficult to achieve today, and, with an expansion of the nuclear industry worldwide with fleets of standard Generation III plants ordered on a 'turnkey' basis, will be even more onerous in the future.

4 Vendor Role

The role of the original plant vendor is therefore important. Often it is the vendor who retains the detailed knowledge of why the design is how it is. Designers should be involved to a greater extent in keeping and improving the safety of a design during operation.

In general, the distribution of responsibility for design change management varies by the safety classification of a system, structure, or component (SSC). When the plant is first built and during its early years, the responsibility of the original NSSS designer for the design change of safety-related SSCs and those important to safety is significant. This was the case with the construction of 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).

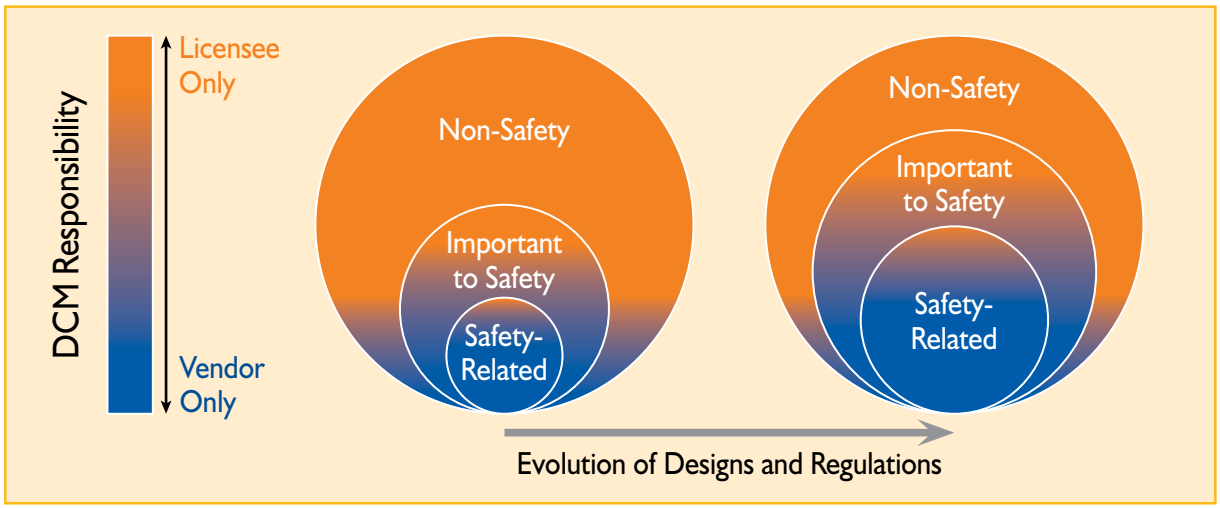

Figure 1. Increasing number of safety significant SSCs with the evolvement of regulation.

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

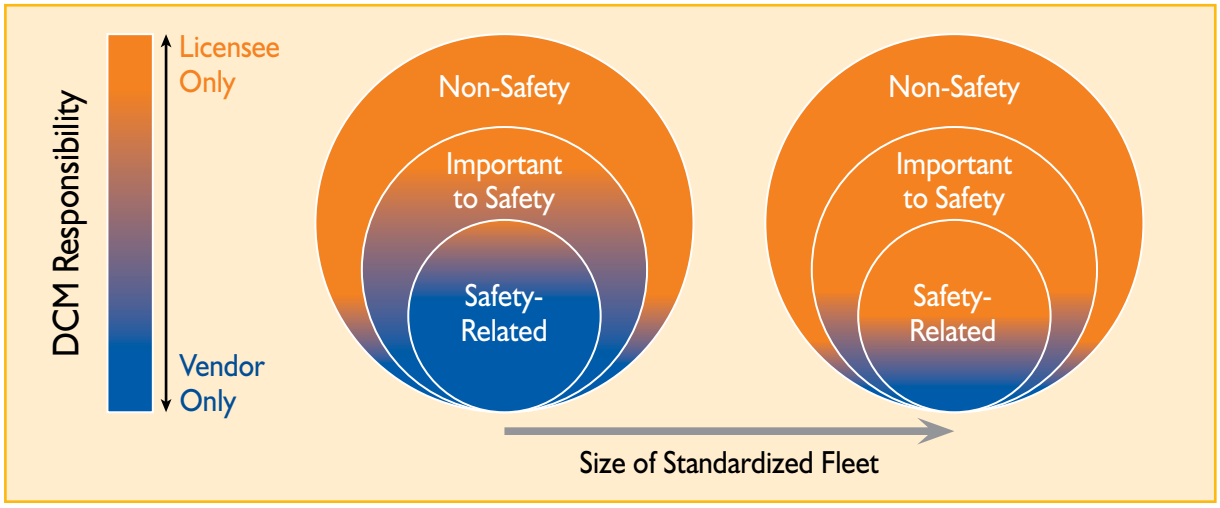

Figure 2. Increasing licensee's ownership of design basis with the increase of licensee's standardized fleet size.

So 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 requires support from the original designer.

These charts simply demonstrate historical precedence for licensee ownership of design basis. This concept might also be applicable in the future in the event a licensee (or country) builds a sufficiently large fleet of the same standard design. India is a good example with future plans for multiple units of a standard design of imported technology. In such a case, the licensee may very well 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 degree of ownership tailored to the capability of the licensee's Design Authority.

For standardized reactor designs the responsibility of the vendor/designer in the fleet oversight internationally should increase. Vendors, in close collaboration with utilities as 'intelligent 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 initiating design improvements which might result from this experience feedback.

The role of the designer should include the compilation of operating experience, in terms of failure modes and failure rates of similar components in a fleet, throughout the lifetime of the fleet. This should include the distillation of operating experience that has implications for design and potential design changes reported through a strengthened 'Service and Advisory Bulletin' system. The compiled data could be far more detailed and valuable than is available today when the cost is spread over the whole fleet. Currently, every utility is expected by the regulator to maintain such a database independently.

The use of 'Service and Advisory Bulletins' on both safety and operational matters needs strengthening and should include a graded approach which reflects their safety significance. The most important should be considered mandatory, as they are in the aerospace business.

Most vendors have developed or are developing inside their organization what some call the vendor's own 'design authority'. It is a group of engineers who keep the history of the various designs they have produced and all the reasons behind the design choices made. Their role is to review any changes proposed to/by their customers to check their 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) but currently it has no direct responsibility.

In the case of the vendor's business being transformed, changing ownership or ceasing to exist, it is important to ensure that the designer's IP assets (including its human resources) are maintained and transferred to another responsible organization that has the technical capability. This could be a relevant Owners Group.

This issue is discussed further in the next section.

5 Owners Group Role

Today, the Owners Group (OG) is a good point of interaction between a vendor and the utilities that operate the vendor's design. Operating experience is shared, as well as common technical issues and the way to solve them.

A high-level assessment and comparison of OGs has been undertaken by means of a questionnaire, involving:

- AREVA Owners Group (Formerly the Framatome Reactors Owners Group, 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's plants)
- Boiling Water Reactor Owners Group (BWROG, GE-Hitachi)

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 and the situation of a single utility linking back to the vendor 'mother country' was also covered. These circumstantial differences could be the cause of many operational differences.

Usually the OG membership is voluntary and assumes no responsibility from the vendor to recommend standard solutions or to influence utilities to implement them.

But some clear strengths and good/best practice can be identified from the survey. It is intended to take this work further and to hold further discussions and develop a good/best practice OG operational model.

The results of the questionnaire can be summarized in the following points:

- **Participants:** All OGs include the vendor(s) and utilities operating this vendor's reactors.
- **Voluntary or mandatory utility involvement:** In most cases, involvement is voluntary but there is one case in which the national regulator mandates involvement with the original designer (in Russia). In some cases, utilities are motivated to join by the membership benefits offered. There is no mandatory requirement for membership at international level, with the exception, perhaps, of the VVER operators in the ex-USSR (Ukraine), where the national regulator demand mandatory adherence to the safety recommendations emanating from the original designer.
- **OG charter:** Most of the OGs questioned have a relatively detailed charter which the member utilities sign up to. In some cases, only utilities are voting members, while the vendor is not allowed to vote (COG, FROG).
- **Primary areas of activity:** There is much commonality in terms of sharing operational experience, reviewing common safety and reliability issues, reviewing common regulatory issues and even plant economics. In some cases this extends to shared research and development to address issues. One of the positive features of OGs generally is the flexibility with which the operational experience (OPEX) can be shared – the sharing mechanisms can be arranged around design-specific features or around a specific secondary supplier's issue who would be attracted to participate only in the relevant activity. The activities can be private; the participation is voluntary where cost sharing is involved, for example.

- **Library of licensing and safety issues:** There were variable responses to this which included several "none" responses, although in such cases there was normally an alternative of some form, e.g. availability of a website that lists common issues and results of analysis (most OGs), providing advisory bulletins (COG), vendor's support can be delivered via televised conferences from vendor's crisis centre (in Gidropress).
- **OG accountability for plant licensed design and analysis:** Generally the OGs, as expected, do not accept any accountability.
- **OG accountability for plant configuration management:** Generally no accountability accepted but there were 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 change management:** Generally none accepted.

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

a) It would be worth considering introducing in the OGs' mandates an objective to adhere to standardization, i.e. if a design issue is identified by one of the OG's members, all members should seek the issue's resolution and its implementation jointly.

b) It is considered that the OGs should define a process to ensure that the detailed knowledge of design differences is accounted for between all plants in the fleet. This should also involve the vendor.

c) Cost/benefit analysis is a good tool for a utility to decide whether or not to make modifications in their plants. Probabilistic Risk Assessments (PRAs) are a basic element of this tool and similar plants (even if not standardized) should have similar risk profiles, provided that the data input into the PRA is coming from a common database. This is another area where the OGs could develop standard PRA techniques related to their relevant designs and collect reliability data from utilities operating these designs as input to PRA. This would allow the vendor to demonstrate the common benefit of a modification to all utility customers and to help avoid implementation of differing technical solutions thus supporting standardization. This concept has already been demonstrated by the US NRC Reactor Oversight Program. In that 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.

d) One of the major issues to agree on and manage, given the longevity of a nuclear plant, is how the design knowledge should be maintained if the original designers are no longer accessible (for example, are 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 a 60 year life. The duties, competencies and responsibilities of replacement design organizations must be well defined and understood at the time of takeover. If no new design organization is available to take over the responsibilities and assets of the designer, the Owners Group could step in to provide a solution for the whole fleet as a last resort.

CORDEL's recommendations propose an evolution in the relationship between vendors and utilities within OGs. The exchange of information between different members of the OGs (utilities and vendor) should be increased in order to achieve the goals discussed here. OGs would all have to make appropriate changes in their mandates based on their own specific circumstances.

The role of the US Nuclear Energy Institute (NEI) should also be noted. The NEI is *de facto* an Owners Group. NEI has an international roster of 350 members in 15 countries and serves as an effective and significant common point of interface with the US regulator on nuclear industry initiatives. For example, there is a New Plant Working Group within NEI, which encourages standardized approaches in licensing of new plants. This group supports the new plant consortia activities in order to enable new plant combined construction and operating licenses to be issued within the time frame needed by member companies. It would be good to see such standardization-supporting activities continuing throughout the lifetime of the plants after they enter into commercial operation.

6 Utility Role

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 is unlikely that they have sufficient engineering resources to know, in every detail, the design they operate and all the reasons behind the design choices made by the vendor. However they should have developed sufficient knowledge of the design to be an 'Intelligent Customer' but even this could be a large undertaking for a small utility. 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, but this would require long-term agreements with commercial implications. There are several examples in which a utility, making modifications on its own, or choosing another vendor to make a modification to improve its performance, has experienced negative consequences.

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 owner's 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 on its own contributes to keeping the units similar. In the context of new build, several US utilities have applied for Combined Construction and Operating Licenses to build same few designs. NEI New Plant Working Group, as mentioned above, was set up in order to facilitate and speed up the licensing process, which supports standardization during the licensing process. At least at the licensing stage standardization will be achieved. The utilities should be encouraged to continue this kind of cooperation beyond licensing stages and during the life of their plants.

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 does not end after plant start up. Some form of contractual agreements should be put in place on a long term basis to ensure the knowledge management of the design. 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 not underestimate the importance of the original designer in design change management, which was recognized by INSAG-19 but no concrete solutions were identified.

Utilities should recognize the benefit of participation in the Owners Groups and should make maximum use of cooperation with their international peers within OGs and within international organizations such as WANO.

7 WANO Role

The World Association of Nuclear Operators (WANO) is a well-established and recognized organisation 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 Report) and SERs (Significant Event Report) that are widely distributed among its members are extensively used by most operators.

In the past there have been very few links, if any, between WANO and vendors. The current WANO policy, however, makes it possible for the nuclear vendors to get access to WANO operating experience information, based on a bilateral agreement including a confidentiality clause and a fee for access to WANO intellectual property.

This is an encouraging development which could progress further. When a significant event exhibits a root cause that is a design issue, interactions with the original vendor should necessarily be made, and the vendor should receive the event report as a rule.

It is not the role of WANO to propose means to solve the identified problem, but through such an exchange the vendor could make use of the analysis made by WANO and propose a common solution to its customers in the most efficient way.

Through its access to worldwide operating experience, WANO is developing reliability data bases. Vendors' access to relevant areas of this information would help improve their PRA quality for the overall benefit of safety.

These recommendations are also applicable to INPO (Institute of Nuclear Power Operations). This organization has all US nuclear utilities, some suppliers and many utilities outside the US in its membership and serves many of the same purposes as WANO, but also includes initiatives to improve plant reliability and evaluations of systems and equipment conditions.

8 Regulator Role

Regulators have begun to make efforts to harmonize their activities and share their assessment 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 standardized solutions during plant life.

The CORDEL roadmap postulates the achievement of joint or coordinated certification by regulators (referring to Phase 2 and 3 of the CORDEL 'roadmap' paper). In such circumstances it could be envisaged that the safety documentation could be distributed in two or three tiers – the first one having the basic safety demonstration and the others containing more detailed description and evidence. Any change affecting tier 1 documentation would have to be reviewed and approved jointly by the regulators with a similar process as for the initial certification process. However, there is a long way to go from initial moves for harmonization through to completely joined or coordinated certification with many obstacles including sovereignty issues, but the industry should continue to encourage progress in this direction.

One concept that has been discussed, potentially as a long-term end-state for MDEP, is the formation and maintenance of 'Regulator Owners Groups' in which multiple regulators meet periodically and share operating and regulatory experiences with a common design.

Examples of such regulatory groups exist – the CANDU Senior Regulators' Group and the VVER Regulators' Forum. Alignment of the charters for the two 'owners groups' (operators and regulators) could ensure timely and cost-effective implementation of regulator-imposed design changes with additional assurance of a consistent design across multiple regulatory frameworks.

Also, this is already the case with the so-called 'EPR family' (an EPR Owners Group that is led by the licensees and includes the original designer AREVA) interacting regularly with the EPR Working Group (EPRWG) of MDEP. This OG works on harmonized solutions to generic issues, keeps track, with the support of AREVA, of the departures between the EPR projects and together with the regulators within MDEP's EPRWG addresses the causes of these departures and works on how to solve them.

Given that progress in making necessary reforms is likely to be slow, there are some actions which may help avoid design divergence of existing similar plants under regulatory influences and can be undertaken now. The Nuclear Energy Agency (NEA) of the OECD, and more specifically its Committee for Safety of Nuclear Installation (CSNI) and the Committee of Nuclear Regulatory Authorities (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 and the Forsmark event which are good examples that helped regulators share a better understanding of the event, the kind of lessons to be learnt from the event and eventually to take more 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 more systematic manner.

Most utilities are looking for life extension of their operating plants. Some regulators, especially in Europe, are taking this opportunity to issue new safety requirements that could result in design modifications and further differences in similar plants. Besides the fact that these new national safety requirements could impair fair commercial competition between utilities, it would be a retrograde step 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 regulators should work together on this issue and both OECD/NEA and IAEA should play a persuading role.

For the benefit of safety and standardization of plants during their lifetime, regulators should develop a consistent requirement for Periodic Safety Reviews (PSRs) to include international experience feedback and to consider vendor recommendations in support of safety improvements. These PSRs, in turn, may produce new relevant safety-related recommendations, which would then be passed onto the vendor and other utilities through OGs or other OPEX exchange mechanisms, such as WANO.

And generally, regulators should demand from licensees mandatory membership in OGs, compliance with OGs recommendations, and consideration of 'Service and Advisory Bulletins' issued by vendors, based on a graded approach in relation to safety importance.

9 Design Authority

The subject of Design Authority has occurred in several places in the paper already and is a clear theme that runs through the whole issue of design responsibility and design change management. The principle of the operator owning the ultimate responsibility for the design of the plant infers that the operator is the 'authority', the decision maker, but the other connotation of the word, implying expert or knowledge holder, refers to a vital capability which may be difficult for an operator to fulfil.

The original vendor of the plant may be in the best position to fulfil this latter capability but this is not guaranteed unless there are 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.

A survey, again by questionnaire, has been carried out by CORDEL to understand currently how different operators are approaching the subject of Design Authority (DA). This covered five countries, 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 Design Authority executed?
- What is the role of the original designer?
- What are the DA accountabilities for design change and configuration management?
- How does the DA ensure fleet wide conformance?
- How many full time equivalent staff are in the DA organization?

The results are summarized as follows:

- **In Korea**, the DA for operating and new plants is a formally designated entity, called the Central Research Institute, which lies within the operator's organization (operator is KHNP). KHNP has continuous access to the 'responsible designers' (RD) – that is the original plant vendor KEPCO E&C and the component supplier Doosan. KHNP delegates detailed areas of the overall DA responsibility to the RD. Repeat projects are increasing the KHNP in-house DA capability. KHNP and KEPCO E&C are both subsidiaries of the government-owned parent company KEPCO, which simplifies matters. KHNP gets support from membership in OGs of overseas vendors for its CANDU and Westinghouse designs as well. 'Responsible designers' hold DA 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 DA is maintained by KHNP with the 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 DA. This model, of operator and designer being part of one company, of obligating the vendor/original designer to both play roles in the DA, and of the increasing DA capability through succession of standard projects, is deemed to be most successful and is worth further study in seeking the ideal solution to the DA issue.
- **In France**, EDF is the operator and architect-engineer of its plants (EDF does not buy turnkey). EDF incorporates within its organization a body called Nuclear Engineering Division (DIN) whose role, among others, is the DA, although the DA role is not formally established. DIN is a senior level division which also coordinates allocation of design-related activities among various EDF engineering centres, such as SEPTEN. A contractual relationship with the original vendor (AREVA) is maintained, but EDF has developed its own "deep knowledge". EDF always seeks to incorporate international experience feedback during Periodic Safety Reviews, and some urgent actions get 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 is not easy for others to adopt a capability of the size of EDF, which has been built over a long period. But there are lessons to learn, particularly in the consistency of EDF's design change management approach throughout its fleet.
- **In the USA**, dependence on the original designers (NSSS vendors) is recognized, as they are current IP owners. Also, Original Equipment Manufacturers (OEM) and OGs sometimes develop design modifications and these have resulted in design change in older plants having been implemented in a different way based on the licensee's own responsibility. In the future, a more clearly defined "joint ownership" of design basis between the operator and designer is 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 current organizations. The role of DA is invested in an individual, supported by a team whose aim is a "full technical understanding" of the plant. There is some evidence of difficulties in some DA areas. In problem areas, delegation via clear contractual agreements with responsible designers is undertaken.
- **In Canada**, the DA is the Chief Nuclear Engineer within the licensee's organization. He may formally delegate some aspects of DA to plant engineering and to a 'design agency' but not overall accountability. Requirements for this process and role are captured formally in RD-337 (based on IAEA SSR 2/1) and in the license itself. For the new build in Canada, the roles of vendor and operator, and the transition of DA from vendor to licensee during handover, are being clarified.

It is clear that there are many common experiences in different organizations but many subtle differences due to, not least, different maturity levels and situations.

Further work is required to pull out all the learning. The aim is to make recommendations for a Design Authority guide. This will include key issues around the need for the DAs within operating companies to have a strong link with OGs, and also with the vendor through commercial operator-vendor relations. Further discussions with regulators on the subject of vendor involvement in the DA should also be conducted.

10 The Aerospace Industry Model

In the addition to the ideas developed in the CORDEL 'roadmap' report [6], further discussions have been held with aerospace industry representatives on the basis that they also operate in a high technology area in which reliability and safety of products are vital.

The aerospace industry developed techniques for adhering to standard designs at international level many years ago. There are several lessons to be learned from this industry, which will be covered by a separate report. These include:

- 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 (Airworthiness Directives and Service Bulletins);
- Interfaces of responsibilities and allocation of risks and liabilities among designers, manufacturers and operators;
- Execution of DA role by manufacturers;
- Industry joined processes of standards development and manufacturer's certification;
- Maintenance of the responsibility of national regulators in an internationally agreed framework.

11 Conclusions and Recommendations

Standardization is mainly seen as a tool to improve nuclear plant economics during design approvals, licensing and construction. But standardization can also bring significant benefits to safety of nuclear power during operation as it offers a wide international basis for experience exchange from the entire fleet of standard plants worldwide. In order to retain 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 design standardization throughout a fleet's lifetime. CORDEL's main focus has been on future new build plants where the opportunity for standardization is greatest, but some of these recommendations are also applicable to existing fleets.

In this report, CORDEL's main findings and conclusions are:

- The Fukushima accident provides an example of institutional problems – there is a lack of an internationally agreed mechanism that encourages design changes to a fleet of similar plants to be similar. This results in a divergence of the design of similar plants over their lifetime which can lead to increasing difficulties in learning from each other. This is counter-productive to safety and will make it more difficult to achieve the reduction in accident probability that is sought for the future.
- The likely global expansion of nuclear power, together with global sales of a small number of turnkey Generation III designs will result in fleets spanning a number of utilities and countries. Those utilities, particularly smaller ones, with limited engineering resources may experience problems in delivering/implementing their Design Authority (DA) role.
- INSAG-19's demand for the utility's accountability for nuclear safety – and therefore for plant design basis through the Design Authority – is not being challenged here.
- The ability of all utilities to discharge this accountability at the level of detail of knowledge needed to make design changes to the plant in all circumstances, without support of the original designer/vendor, is being challenged. Reliance on the plant vendor will be necessary in many situations.
- The existing mechanism of the Owners Group (OG) already provides a good point of interaction between a vendor and utilities with the potential for major assistance in design standardization. However, OGs are mainly based on voluntary utility involvement. Opportunities and benefits for mandatory membership of all the utilities operating the 'same' design should be reviewed and strongly encouraged by their regulators.
- WANO interaction with vendors and OGs could provide substantial benefits in relation to design issues resulting from operational experience. WANO has already started involving vendors and is currently considering further policy changes.
- There is also limited but successful experience of 'Regulator Owners 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.
- Initial discussions with the aviation industry have identified some key areas of potential common interest.

The following recommendations are made to address concerns raised in the above conclusions and to pursue the benefits of design standardization in general:

Design Change Management and Design Authority

1. **A regulatory framework agreed internationally between national regulators** that requires, for each situation, a clear definition of roles and responsibilities of the vendor in the international design change management process and how the vendor is managed by the utility in discharging the Design Authority role, should be developed.
   - Generation III vendors will be in a unique position to assess proposed design changes and make design change recommendations. This vendor's role must be defined in vendor-utility agreements which should include initial design information handover and the potential for changed circumstances of parties during the life of the plant.
   - The focus of these agreements must be to maintain design standardization, with benefits of standardization being given full weight, in all design change decisions with best practice being shared internationally.

2. **A Design Authority guide**, identifying best practice through working with utilities and vendors, should be developed.
   - This should include a definition of Design Authority that can survive and work in many different utility/vendor/regulator scenarios. This should cover how the role of DA, which rests with the operator, can be enhanced and made to work across different organizations with different organizational structures and commercial arrangements, and without resulting in an unnecessary cost burden.

Owners Groups

3. Further, 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 applying peer pressure on those non-conforming and by demanding justification for alternative solutions.
   - Strengthening the involvement of the original vendors in OGs, including the use of vendor 'Service and Advisory Bulletins' within the OGs.
   - Strengthening the role of the OGs, with respect to identification of significant safety issues, which then should result in recommendations to be adopted by all OG members.
   - OG production of reliability data and a standard Probabilistic Safety Assessment for a design.
   - The production of a OG best practice guide.

WANO

4. Further discussions with WANO about strengthening its role is recommended. These should include:
   - WANO's relationship with OGs should be developed where OGs could help produce reports on design-specific issues for dissemination among participating utilities.
   - Involvement in the development of a worldwide reliability database, which could be further strengthened by design-specific reliability data accumulated by OGs.

Regulators

5. The benefits of design standardization to safety throughout life should be recognized by regulators. Regulators might consider:
   - Setting up 'Regulator Owners Groups' and task forces and conducting workshops for specific emergent technical problems.
   - Considering mandatory licensee membership in OGs and compliance with OG recommendations.
   - Setting up an international process that takes into consideration vendor 'Service and Advisory Bulletins', based on a graded approach in relation to safety importance.
   - Developing a consistent requirement during Periodic Safety Reviews (PSRs) and lifetime extension processes to include international experience feedback and to consider vendor's recommendations in support of safety improvements. In turn, these PSRs themselves should also produce new relevant safety-related recommendations, and these could then be passed onto the vendor and other utilities through OGs or other OPEX exchange mechanisms, such as WANO.

Other Industries

6. Further discussions with the aerospace industry are recommended and a regulator seminar to assist this should be considered. These discussions should include:
   - The areas of regulatory harmonization and DA management, which are two of perhaps many areas where there is a potential to learn.
   - Lessons learned from the Type Certificate process and the interfaces of responsibilities.

REFERENCES

1. INSAG–19 *Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life*, IAEA, 2003.
2. IAEA Safety Standards, Fundamental Safety Principles, No. SF-1, Principle 1: Responsibility for safety: *"The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks"*, IAEA, 2006.
3. Convention on Nuclear Safety, Article 9: *"Each Contracting Party shall ensure that prime responsibility for the safety of a nuclear installation rests with the holder of the relevant licence ..."*, IAEA, 1994.
4. IAEA Safety Standard, Safety Requirement, No. SSR-2/1 *Safety of Nuclear Power Plants: Design* (revision of Safety Standards Series No. NS-R-1), Requirement 3 Safety of the plant design throughout the plant lifetime: *"The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the plant lifetime"*, final draft as per January 2012.
5. WNA, CORDEL WG, *Benefits Gained through the International Harmonization of Nuclear Safety Standards for Reactor Designs*, 2008, http://www.world-nuclear.org/uploadedFiles/org/reference/pdf/ps-cordel.pdf
6. WNA, CORDEL WG, *International Standardization of Reactor Designs*, 2010, http://www.world-nuclear.org/uploadedFiles/org/reference/pdf/CORDELreport2010.pdf

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.

World Nuclear Association
Carlton House • 22a St. James's Square • London SW1Y 4JH • UK
tel: +44(0)20 7451 1520 • fax: +44(0)20 7839 1501
www.world-nuclear.org • info@world-nuclear.org