Nuclear Regulation and Gen III Reactors

J G Waddington, B.Sc., P. Eng.

Nuclear Safety Consultant

johnwadd@magma.ca

Abstract

The paper discusses the challenges that reactors with a 60 year lifetime, licensed in many countries and operated by many utilities, present to the regulator. Issues of international standards, technology neutral regulation, design responsibility, configuration control, balancing sources of risk and their review, regulatory efficiency and cooperation, and integration of regulatory observations over time and space will be discussed.

Introduction

The increase in electricity generation from nuclear energy that is expected to occur over the next decades will put great strains on the design, manufacturing and construction capabilities of the nuclear industry world-wide. It will also challenge the regulators of the world to come up with better ways of ensuring even higher levels of safety at far less cost and time, if the opportunity of nuclear power to provide clean, cost effective energy to many countries around the world is to be realised.

The Renaissance

We are all aware of the expectations of the nuclear renaissance. The International Energy Agency predicts that the number of nuclear reactors in the world today may double over the next 20 to 30 years, with much of the expansion in Asia. That's 300 to 400 new reactors. Lest anyone have doubts, I note that the USNRC has already received applications for 23 new units, with another 11 expected over the next 2 years [1]. The ageing of power stations in the western world; the widespread understanding that we have to get really serious now about the effects of industrialisation and energy use on the world's environment; the need to drastically curtail carbon dioxide and GHG emissions; the dramatic expansion of Asian economies, particularly China and India; and the desire to reduce reliance on volatile parts of the world for sources of energy have come together to produce a "perfect storm" of an expansion; an enormous pressure for the development of environmentally friendly sources of power in the immediate future. The

International Energy Agency notes that it is not capital that we lack in facing these challenges- it's time [2].

I would like to present to you a number of issues that this expected expansion will bring to the industry and to the regulatory agencies in particular.

Standardisation

It is reasonable to assume the generation III reactor designs that are available now will provide bulk of these numbers. Let us assume that there are, say, 10 designs available on the world market. Let's further assume that the 300 to 400 reactors are made up of 20 copies of the least popular design, and, say, 50 copies of the most popular design, each spread around a ten or more countries

Clearly, the nuclear business has entered the age of mass production. To achieve this situation at reasonable cost, designs must be standardised-, not just the core but the whole plant, given that we know that the achievement of a very low probability of a severe accident is dependent on the whole plant, not just on the components of the nuclear island, and as a result the whole plant is part of the licensing process. There are not enough people available in the regulatory agency of any country to both monitor the safety of the existing fleet of reactors in their country, as well as do detailed reviews of many non-standard designs, and I doubt any utility in the world wants to spend the cash on a one-off.

None of this is new; the USNRC understood this issue 20 years ago, and put in place a design certification and licensing process to deal with it well ahead of the demand [3]. The UK and French Governments both asked the IAEA to look at adequacy of their nuclear regulatory systems when faced with this expansion, and the IAEA recommended that in both countries, the informal pre-licensing review that has been the most common way for regulators to start looking at new designs be changed to a formal process leading to design certification [4,5]. The French Government has already changed their legislation to allow for that [6]. It's well past the time when we followed the same route here in Canada, and changed our regulations to give legal authority to the CNSC to issue a formal design certification. We will discuss this issue more in a moment.

The Perception of Safety

A few years ago, the aircraft business faced a similar expansion issue. They expected a doubling of the number of passengers traveling by air over a period of several years and hence a nearly doubling of the number of planes flying. All things being equal, it was reasonable to expect that

the number of planes that fall out of the sky each year would also double. Twice the number of reports of crashing aircraft in the newspapers did not seem to be good PR, and the airline industry wanted the number of actual accidents to stay the same; - i.e. they were looking to halve the accident rate. They recognised that much effort was needed to achieve this, and in the intervening time they have put much effort into SMS- or Safety Management Systems -safety culture to us.

Expansion will bring more safety issues to the nuclear industry too, and we will have to follow the lead of the aircraft industry. To quote Dr Nils Diaz's speech at a conference in Moscow two years ago [7], many countries with no past experience with nuclear power have expressed interest in building nuclear power plants. These countries include Belarus, Egypt, Indonesia, Malaysia, Turkey, Poland, Vietnam, Nigeria, and various countries in the Middle East. Even if a foreign vendor is responsible for the design, construction, and commissioning of a plant, the recipient country has the obligation to ensure the existence of a strong infrastructure that can guarantee continuing attention to safety for a period as long as a century or more. There are many components of the necessary infrastructure, including legal and regulatory capability, educated and trained manpower, a stable electrical grid, access to financial and industrial resources, and the nurturing of an appropriate safety culture in the generating entity.
In other words, the regulators and operating organisations in new countries will need to develop high levels of knowledge of operations and of how to achieve a high level of safety, including safety culture. I contend that they do not need a detailed knowledge of reactor design to do this. We will discuss this too in a moment.

The Design Authority

In the early 1990's a letter was received by the IAEA's Director General from V P Bryukhanov, the Station Director of Chernobyl. As I remember, his letter started out "I have just been let out of prison after 4 years". His letter took issue with the IAEA, who, in their initial assessment of the Chernobyl disaster, put the onus for the accident squarely on the operator. His objection was that, as station director, he was not responsible for the design faults in that reactor, notably the combination of a large positive void coefficient, a positive temperature coefficient and the positive reactivity that occurred in the reactor when the shut off rods were first inserted. With hindsight, there is no doubt that the operators at Chernobyl made significant operating errors that made a big contribution to the disaster, but Brukhanov had a point. Should he have been held responsible for design flaws in the RBMK reactor? How could he be?

In a certified design, when the reactor designer has obtained a design certificate from the regulator that a potential utility can use to substantially shorten the site and operating license processes, what responsibility does the operator have for the design itself? If a design weakness

is discovered, whose responsibility is it to ensure all 20 to 50 other plants around the world of the same design have the weakness corrected? In say 10 different countries? If a design change is required as a result of an incident, who decides if that design change must be duplicated on all other copies of the design? When a design is changed, is it still certified? Or if a design isn't changed when it was supposed to be, is it still certified? Who decides, and on what basis? Who makes the application? Clearly, there are many more issues to design certification in the Generation III world of multiple copies that just making the licensing process more efficient, important though that is. In a mass produced product, I submit that must be the designer. Would you accept Air Canada was responsible for the design of the plane you are flying in? No you would not. It's Boeing. Or Airbus.

Maintenance of Design Knowledge

In the early days of the nuclear business in Canada, the design was shared between the reactor designer, AECL, and the utility and architect engineer, Ontario Hydro. The conventional wisdom is that the design of Pickering was 80% AECL, 20% OH; Darlington was 20% AECL and 80% OH; and Bruce was somewhere in between. Ontario Hydro had a large design staff to deal with this.

That design staff has largely disappeared from Ontario Hydro. The small utilities never really had them, though even they were operating with a staff ratio of about 1 "Full Time Equivalent" person for every MW generated. For Generation III reactors, this ratio needs to drop to 0.75 FTE's /MW, or even perhaps to 0.5 FTE's /MW to really make a dent in operating costs - and to make it possible to find the qualified people needed to run and maintain all these plants and maintain their configuration control. To expect every plant to have enough technical staff to be able to capable of maintaining the "Design Authority" responsibility seems a very unwise expectation. Of course every operator must know as part of its operating knowledge the basics of design; the basis for its safety; the equipment and operating configurations that must be respected to ensure a very low probability of serious accidents; and the minimum specification required of all its components. But in the future, they will not be experts in design. INSAG-19 [8] discusses the issue of maintaining the design integrity of nuclear installations throughout their operating life and notes:

Nuclear power plants are complex machines. They are composed of many interdependent systems which must operate in a manner that meets the design intent over a period of many decades. This long period of operation means that a plant will undergo change throughout its life. The changes can arise as a result of

- the physical ageing of the plant's systems, structures and components;
- the obsolescence that inevitably occurs in many of its hardware and software elements;
- feedback from operating experience

- research on unexpected design issues arising during its life;
- changing engineering or regulatory standards;
- changes in performance expected from the plant; and
- changes in the organization or practices of the operating company.

To maintain the very high level of safety expected of a plant requires that design changes arising from these or other sources must be made with a full understanding of all the design information for the plant and the specifications for each system and component; of the engineering compromises and assumptions made by the designers about operation and lifetime; of why the plant was designed the way it is; and of the interactions with other systems and components which could affect safety.

INSAG-19 also notes:

- The accessibility of design knowledge is not a trivial matter. The amount of data is huge, as it includes, for example, original design calculations, research results, mathematical models, commissioning test results and inspection history. Further, many design change issues can be complex.
- Failure to ensure full knowledge of how plant design is maintained and to manage design changes adequately will, over the lifetime of the plant, result in decisions being taken on modifications, back-fits, changes in operating procedures and specifications for spare parts without a full understanding of the effect that these decisions may have on the safety of the plant. Unintentional consequences that could affect the safety of the plant are likely to occur in these circumstances, and the possibility that an accident could happen as a result will likely increase.

INSAG 19 identifies the need to maintain the knowledge of a design in order to maintain the design integrity of the plant over its entire lifetime [8]. This may be achieved by setting up a Design Authority within the operating organisation, or by having a formal relationship with the original design organizations or their successors as Design Authorities. Given that, for Generation III reactors, operating organisations are unlikely to have a design capability, what is the role of the operator here?

The UK Health and Safety Executive have a lovely expression for it. The Operator must be an “intelligent customer”. Now most operators in this room would say- quite rightly- “We are- and we don’t need a regulator to tell us that!” But the UK HSE does clarify what it means [9]. Briefly, a Licensee who is an intelligent customer requires technical expertise that gives it:

- sufficient expertise to understand and support the safety basis on which the Licensee operates;
- knowledge of the limitations and boundaries of the safety cases and of how these may change over time, or as circumstances change;

- the capability to oversee and, where necessary, develop and determine relevant safety and engineering standards, and to ensure the standards are met.

It seems to me that the nuclear renaissance is unlikely to expand very quickly if the level of technical support needed to maintain the responsibilities of full Design Authority for a Generation III design is expected to be retained by the staff of the nuclear power station or its parent utility.

Regulatory Expectations

Regulatory agencies around the world uniformly state "the licensee is wholly responsible for safety". Liability legislation in every country says so. Hence the regulator holds the operator fully responsible for the design as well as for operation. When I joined the AECB (now the CNSC) in 1975, the designer was considered to be just a contractor to the utility, with no responsibility for safety at all. As an aside, one consequence of this thinking in Canada, is that questions of design and analysis that remained after the current fleet was licensed- known to you all as Generic Action Items - have taken for ever to resolve. The CNSC required the utilities to solve them, since they were the holders of the licence, and the designer was not held responsible by the regulator at all.

In the early days of the nuclear power program, governments wanted to get the industry up and running, and didn't want the man in the street to have to say "who do I sue if my home is contaminated by a nuclear accident". Hence the Nuclear Liability Act in every country makes the operator wholly responsible for the results of any accident. Regulators have taken this to mean that operators are responsible not just for operational safety, but also for all aspects of the design. The legislation in every country was written to licence just the operator, and hence the regulator only had the holder of the operating licence to deal with. And after all, the licensee is the organisation that's making the risk–he's operating the reactor, right?

From an engineering and real safety point of view, the idea that, once the plant has been handed over to an operator, the designer has no formal responsibility for the design is, in my view, nonsense. As we have seen, the operator is responsible for operating to specific equipment and system specifications, operating limits and configuration control; the designer ensures robustness of design and defines the minimum performance required of systems important to safety. Operators of Generation III reactors will not have all the knowledge and expertise to be able to meet the expectations of the regulator that they maintain responsibility for the design throughout life. They must instead be "intelligent customers".

So- just as we are on the brink of a dramatic expansion of nuclear power that the world REALLY, REALLY NEEDS, world-wide our regulatory model is based on an assumption which in the past was unsatisfactory, and in the future will be pure fiction.

This is no basis to maintain high levels of safety all around the world.

The USNRC- as usual- has shown the way to solve the problem. It's Design Certification, and regulatory cooperation.

Design Certification

The USNRC introduced the concept of Design Certification 20 years ago to recognise two imperatives to reduce licensing costs; the early review of new designs, and the need for standardisation. In 1988, the NRC issued NUREG-1226 [10]. The NUREG provides guidance on the implementation of the policy and describes the approach used by NRC in its review of advanced reactor design concepts. We now have to go further than NUREG 1226.The size and urgency of the renaissance requires regulators and the industry to sort out the questions about Design Certification and Design Authority that we have raised in this paper. Here are some more issues. If a design is certified in one country and the regulator in another country wants to change it, is it still certified? Who sends the letter out to the operators of all the plants to say- you HAVE to put in a design change?

These are not new problems. Again, the aircraft business solved all most of them years ago, and we can learn from them. But nuclear regulators have to recognise the issues and put the necessary processes in place, including the international treaties and changes to national legislation that will eventually be needed.

There are many hurdles. The main one is the recognition by the regulatory agencies of the proper balance of responsibilities for safety between designers and operators. This need NOT change at all the public responsibilities of the operator defined by the Nuclear Liability Acts. What it will change is the situation that could occur after an accident happens and after any compensation has been paid by the operator's insurance company to the public. If an accident is caused or contributed to by a design flaw, the responsible designer presumably could be sued by the utility after the provisions of the Nuclear Liability Act have been met. It is not clear that such an action would be successful in the current regime.

Rationalisation of Requirements

At risk of annoying Boeing and its carbon fibre Dreamliner designers, it seems to me that there is far greater a variation in the basic design of reactor than there is in aircraft. To illustrate this, compare the difference in basic structure between the PWR and the BWR, the PHWR, and FBR, and then look at the differences between a Boeing and an Airbus. The task of coming up with internationally accepted rules for reactor design will therefore be more difficult for the nuclear business than the aircraft business. But it has to be done. A regulator cannot use a set of design requirements that it has developed for one type of reactor to regulate another type of reactor. Instead there has to be some international agreement on requirements that are specific to the type of reactor. This should be easier to obtain than one set of rules that is intended to be applied to all types.

The IAEA has developed "technology neutral" requirements that can be applied to every reactor design in its NS-R-1 document, "Safety of Nuclear Power Plants- Design" [11], but these are at a very high level. No regulator would use these alone to regulate a specific design. Specific, detailed requirements that are not technology neutral have been developed by every regulator, and are the result of many knowledgeable people's efforts. To illustrate the point, a group of 12 European utilities developed common requirements for just one design- the LWR [12]. There are 4000 requirements identified in this document. Since it was the utilities that developed the document, it covered much more than just safety, but it illustrates the point that you CANNOT LICENSE BY TECHNOLOGY NEUTRAL REGULATORY REQUIREMENTS alone.

Regulatory collaboration to obtain some common recognition of the safety of each design is obviously essential. Nils Diaz and Richard Merserve, both Chairs of the USNRC, have been pushing hard for such collaboration, resulting in the formation of the Multinational Design Evaluation Program (MDEP) through the IAEA [13]. Note that it was originally MDAP- Approval, not Evaluation, but reality- in terms the desire by all regulators to be masters in their own countries, crept in and the goal was scaled back.

INSAG has published a new report, INSAG-21 [14], which makes the case for such collaboration. It notes that:

"The basic goal of a multinational reactor safety review should be to ensure that a design determined to be safe in one country does not have to be substantially modified to meet licensing requirements elsewhere. This can be achieved if the requirements that must be satisfied in one country are consistent with, or at least not significantly different from, those that must be satisfied in another. The importance of this basic goal reflects the general expectations of the public and the industry that fundamental safety principles must be universally satisfied."

The difficulty is that the devil is in the details. There are many different ways of satisfying the fundamental safety principles, and it is not reasonable at the moment to insist on a specific set of international standards. Nevertheless, the multinational review should provide a path to the global harmonisation of safety approaches for each type of reactor.

There is international agreement in the endpoint of the regulatory regime for every design- the risk of a severe core accident has been essentially agreed for new plant at 10^{-5} for core damage, and 10^{-6} for severe accidents, and every Generation III design does much better than that.

To me, this illustrates the way forward to harmonise standards if regulators are really serious about it. Probabilistic Risk Assessment is a powerful tool for looking at the relative risks presented by different failure modes or event sequences, and the efficacy of potential solutions. If the same analytical tools are used with the same rigour to analyse different requirements and their solutions on the same plant, the real contribution to safety of both the requirement and the solution can be compared and understood. This gives a dispassionate route to identifying internationally, for a given reactor type, what different design requirements called up by different jurisdictions really contribution to the safety of a design, and what may be a mutually acceptable solution. An example of the problem to be solved is given by the problems faced by the EPR in Finland. The EPR was designed to criteria agreed between France and Germany, and completed an extensive review process by the French regulatory authority. It is currently being reviewed by the USNRC for design certification. The Finnish regulatory agency requires that a steam generator tube leak should not result in the release of any primary coolant to the environment [15], and AREVA had to make changes to deal with this new requirement, resulting in delays and increased costs. This difference has occurred despite reported collaboration between the regulatory agencies of France, Finland and the US. The Finns also noted additional work would be needed on details of the reactor core design, the reactor emergency borating system, the containment liner, emergency cooling systems and severe accident response. It is essential to the greater goal of ensuring affordable, environmentally sound energy be available world-wide that ways of resolving these differences of opinion be found. The advantage to national regulators of such regulatory collaboration and hard-nosed technical comparisons using PRA, rather than comparisons of regulatory theory, is that their own national rules for each type of design WILL GET BETTER in terms of assuring safety, if they are scrutinised on a factual and results basis. The challenge for the world's regulators is all the greater in that the designs of all the Generation III reactors are nearing completion. There is not much time to get this right.

As an aside, for those who still have difficulty accepting the probability figures from these analyses, please note that the precise numerical values of probabilities arising in PRA analysis is not so important; what is important is that analyses that are to be compared are of the same quality, and represent as logically as possible the real systems of the plant.

Exchange of Operating Experience

This topic is probably the area that has one of the greatest benefits to safety in the long term. Standardisation, recognition of the wider implications of design certification and of the realities of design authority all provide a basis for a marked improvement by learning from world-wide operating experience gained from each fleet. Standardisation should make it much easier to agree on uniform codes to identify common components and their failure modes, uniform definitions of failure categories, and to apply lessons learned. Regulators and designers must be as heavily engaged as operators in the development of uniform and comprehensive reporting processes of failure rates and modes, as all have a vital stake in the results. Regulators particularly will have a far greater possibility in integrating and understanding observations about the real safety of a particular plant and the performance of the operators within its jurisdiction when there is ready access in a common form to a much greater experience base than is available domestically.

It will require a great deal of goodwill, common purpose and effort by the regulators to achieve these gains- but they are worth it.

Conclusions

I have tried to illustrate some of the challenges that the deployment of 300 to 400 Generation III reactors over the next 20 to 30 years will pose, particularly for regulatory bodies world-wide. They are substantial, but they have to be addressed if the expansion is to take place and, at the same time, maintain a high level of safety and even improve it. Underlying all is a recognition by regulators that, in their own interests as well as that of the world community, they have to think globally as well as nationally, and be prepared to collaborate with their colleagues on a scale that has not been seen before. Failure to do so is likely to put a large and unnecessary additional burden on the development of an essential source of energy for the future.

Here in Canada, it is essential that the CNSC start the process to incorporate a formal design certification process into its legislation, and develop the necessary changes to the regulations. I believe the legislative change is not difficult; what will be difficult is changing the underlying regulatory mindset that has been in place for 50 years.

J G Waddington

Canadian Nuclear Society Annual Conference, June 1-4, 2008

31 May 2008

References

1. USNRC website-new reactors-expected new nuclear plant applications-updated June 4, 2008

2. World Energy Outlook, International Energy Agency, 2007

3. US Federal Register 52 FR34884 10 CFR Part 50, Nuclear Plant Standardisation, September 1987

4. Integrated Regulatory Review Services (IRRS) Reduced Scope. Report to the United Kingdom, IAEA, April 2006

5. Integrated Regulatory Review Service (IRRS) Full Scope to France IAEA Nov 2006

6. Law 2006-686 Transparency and Security in the nuclear field Act 13.06.2006

7. Opening Address; Facing Safety and security Challenges; A National and International Perspective. N Diaz, Chairman, USNRC. Proceedings of an IAEA International Conference, Moscow, 27 February- 3March 2006

8. INSAG-19. Maintaining the design Integrity of Nuclear Installations Throughout Their Operating Life. IAEA, Vienna 2003

9. The United Kingdom's National Report on Compliance with the Obligations of the International Convention on Nuclear Safety, Revision 2, September 2001

10. NUREG 1226. Development and Utilization of the NRC Policy Statement on the Regulation of Advanced Nuclear Power Plants, June 1998

11. NS-R-1 Safety of Nuclear Power Plants: Design. IAEA, Vienna, 2002

12. European Utility Requirements: Common rules to design next LWR plants in an open electricity market. Pierre Berbey, Olivier Rousselot, Paper IAEA-CN-114/E-7. Conference on fifty years of nuclear power- the next fifty years. Obninsk, Russian Federation, June 27-July 2, 2004

13. Nuclear Safety Review for the Year 2006. IAEA, Vienna

14. INSAG-21 Strengthening the Global Nuclear Safety Regime. IAEA, Vienna 2006

15. Preliminary Safety Assessment of the new Nuclear Power Plant Project. Radiation and Nuclear Safety Authority, Finland. 7.2.2001