Pragmatic Application of the Precautionary Principle to Deal with Unknown Safety Challenges

G. Frappier, A. Viktorov
Canadian Nuclear Safety Commission, Ottawa, Canada
gerry.frappier@cnsc-ccsn.gc.ca, alex.viktorov@cnsc-ccsn.gc.ca

Abstract

Nuclear power technology has matured over a number of decades to the point where our understanding of the technology under a wide variety of circumstances is quite high. Despite this high degree of maturity, discoveries of new challenges occasionally surface. These may arise from either unusual or unexpected operational conditions or new experimental findings from ongoing research. With the early realization that such discoveries could occur, a conscious effort was made to take precautions against their negative impacts. Principles such as defence-in-depth, designing for high reliability, incorporation of robust safety margins and use of justified conservatisms are key examples of established practices that are embedded in national regulatory regimes of most, if not all countries with nuclear programs. Because of these provisions the safety cases of the current generation of reactors proved to be quite resilient to discoveries of earlier unrecognized challenges.

A fundamentally important element in the management of "unknown unknowns" is a healthy research programme. Such a programme is especially necessary as a pre-condition for understanding potential impacts from changes in operating conditions or implementation of novel design features. A research programme helps minimizing chances of stumbling on "unknown unknowns", and allows resolution of emerging issues to by virtue of the accumulated understanding and capability to predict challenges to safety.

In the few instances when discoveries occurred with recognized negative effects on safety, these spurred changes in operating conditions, maintenance or testing practices, design modifications, as well as required targeted research projects. This paper outlines several CANDU-specific "discoveries" in the field of thermalhydraulics, illustrating past "unknown unknowns" and the actions taken to address those. The main message, however, is to point out that both the industry and the regulator should maintain adequate provisions to deal with "unknown unknowns" and that a constant vigilance is necessary to avoid complacency.

Keywords: safety, precautionary principle, safety challenge, unknowns

1. Introduction

Discoveries of new challenges occasionally occur arising either from unusual operational conditions or new experimental findings. In recognition of such eventualities, a conscious effort was made to take precautions against negative impacts of previously unrecognized challenges, from the beginning of civilian application of nuclear energy.

As practical but still high level interpretation of the precautionary approach, principles such as defence-in-depth, designing for high reliability, incorporation of robust safety margins and use of justified conservatisms were developed and are now applied throughout the nuclear industry. Faced with uncertainties in inputs (and recognizing a potential for existence of unknown unknowns) decision-makers seek approaches that bound the uncertainties (conservatism, safety margins) and provide layers of protection (defense in depth).

Because of these provisions, the safety cases of the current generation of reactors proved to be quite resilient to discoveries of earlier unrecognized challenges and substantial backfits of the plants designs are quite infrequent. The new designs respond to the societal demand for safe technology and systematically apply the safety principles in design, construction and operation.

At the same time, as knowledge accumulates, it has become possible to better quantify previously highly uncertain inputs. In some instances penalization of the design and operation, due to the imposition of conservative solutions, could be seen as excessive and is being relaxed as a function of updated safety cases – revised to benefit the recently gained knowledge. Potentially powerful tools for a wholesome evaluation of various risks posed by complex systems are presented by the Probabilistic Safety Analysis and Risk-Informed Decision Making.

2. Precautionary principle

Many, not necessarily equivalent, definitions of the precautionary principle (or approach) exist. The Wingspread Conference on the Precautionary Principle in 1998 proposed the following formulation:

> *"When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically."*

This is an example of the “strong" version of the principle that does not refer to consideration of costs. Alternative versions, such as the Rio Declaration of 1992, state that:

> *“In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of*

> *serious or irreversible damage, lack of full scientific certainty shall be not used as a reason for postponing cost-effective measures to prevent environmental degradation".*

In this instance of a so-called "weak" version of the principle, the consideration of costs is part of the principle.

In the last decades, the precautionary principle has been widely accepted as a governing principle in regulation of potentially dangerous activities. For example, in Canada, the *Canadian Environmental Protection Act* states the following:

> *... the Government of Canada is committed to implementing the precautionary principle that, where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation*
> …

The fields where this principle has been invoked most are the climate/environment protection as well as health protection. However, the highly generalized nature of the principle makes it applicable in any area of human endeavors where risks are difficult to quantify.

In practical fields, such as engineering, the precautionary principle is often formulated more succinctly. One can hear paradigms such as "Failure is not a viable option in design and operation of a nuclear reactor" or even shorter – "better safe than sorry"! Essentially, this approach was a cornerstone of the safety philosophy in nuclear engineering since the early days, but gained prominence especially after the serious accidents at Three Mile Island and Chernobyl. In combination with other fundamental principles it has been instrumental in ensuring a high safety record of nuclear power plants.

3. Practices in nuclear industry

While being the recognized foundation of the safety philosophy, the precautionary principle is not sufficient in itself to serve as a regulatory requirement; it needs to be supported by more detailed principles and even more detailed technical requirements.

a. Safety Culture

The concept of safety culture was solidified following the assessment of the Chernobyl accidents and it underlying causes[1]. Since then it has permeated essentially all domains of human activities where safety is often influenced by human factors. According to INSAG-4

[1] INSAG (1988) 'Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident'.

> *Safety Culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.*

Safety culture is seen as key premise in continuous drive for improvement and guarding against complacency or commercial pressures. Healthy safety culture in a design or operating organization will not allow thinking that a system is safe simply because no information is available to say otherwise.

b. Defence-in-Depth

Defence-in-depth has been the centerpiece of the current nuclear regulatory regime and is justly expected to remain an essential element in ensuring safety for both existing and new plants. The concept has been distilled, refined, tested and developed into a widely accepted regulatory principle (See, for example, a comprehensive definition and discussion in INSAG-10 *Defence in Depth in Nuclear Safety*). The modern practice requires application of defence in depth to all safety activities, whether organizational, behavioral or design related, to ensure that they are subject to overlapping provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. It is applied throughout the design of a nuclear power plant to provide provisions (inherent features and characteristics, equipment and systems, as well procedures and operational guidance) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. The rigorous application of the defence-in-depth concept ensures that safety will not be wholly dependent on any single element of the design.

c. Safety Margins

As part of safety philosophy, safety margins are incorporated in the design to provide further assurances against failures of functions and barriers. Safety margins provide confidence that, in spite of uncertainties associated with the knowledge of plant behaviour under accident conditions, the plant will operate safely in case of challenges. They also compensate for partial equipment failures and human errors.

The concept of safety margin was introduced in recognition of the fact that uncertainties exist and will always exist in characterization of phenomena and processes that might challenge the plant safety functions and barriers. For each damage mechanism that can lead to the loss of a barrier or function, failure limits will need to be identified from experiments; subsequently in design, safety margins will be applied to arrive at safety limits to be used in design and operation. Sufficient safety margin need to be demonstrated for any scenario covered by the plant design basis.

d. Conservatism

Conservative approach in the design for safety means deliberate selection of quantitative values, assumptions and models such that the evaluated values of safety challenges will be exaggerated and very likely exceed those that would occur in reality.

Nuclear reactor design incorporates a degree of conservatism that is commensurate with the safety importance of a particular system and adequate to envelope for all permissible operational states. In deterministic safety analysis, conservative assumptions are made at all steps of calculations of accident progression to show that the plant and its safety systems will meet safety requirements and that the consequences, in terms of releases of radioactive materials and public doses, are acceptable.

e. Design for reliability (independence, separation, redundancy, SFC)

Design for reliability, as implied by the term, aims to produce a design that will have high resilience against failures, in normal operation as well as when subjected to unusual, but predictable challenges. This approach has developed into a discipline in itself, combining the proven engineering practices with insights from the reliability theory. Possible challenges to the system functioning are systematically identified and designed against, such that in case of any plausible events and partial failures, the safety system will maintain its key functionality. The important techniques include:

- **independence:** failure of one (sub)system will not lead to the consequential failure of another (sub)system
- **separation:** systems that perform same (redundant) functions are physically separate so that they cannot all be disabled due to the same initiating event
- **redundancy:** if one part of the system fails, there is an alternate success path, such as a backup system
- **single failure criterion (SFC):** no failure of single component in a system will completely disable the total system functionality.

This approach allows the designer to propose a system or a complete plant taking into account, and protecting against, all known and plausible safety challenges.

4. Moving from unknown to known

In the section above, we discussed some (not all) principles built into modern safety regulatory framework. A careful reader perhaps noted that those techniques would work well in cases where the safety challenges are known and understood.

From the scientific or engineering point of view, understanding of a system (or a process) is equivalent to an ability to describe the behavior of interest using a mathematical model. Such a model can then be used to predict the system response as a function of changing characterizing parameters.

It is also acknowledged that any model is inevitably a simplification that predicts the system response with limited accuracy over a finite range of parameter values. To put this differently, any model is always characterized by uncertainty which is a quantitative measure of the model fidelity.

Several categories of uncertainty are associated with the mathematical modeling of a system, in particular:

- completeness uncertainty which describes goodness of the mathematical formulations in the model,
- parameter uncertainty which characterizes how closely the values of input parameters used in the model match the reality.

The latter, the uncertainty in values of parameters, is often subdivided further to distinguish the following:

- aleatory (stochastic) uncertainty which is a measure of natural randomness of parameter values,
- epistemic uncertainty which is a measure of accuracy of knowledge of an actual value of a parameter.

We will not delve much into the depths of the fascinating subject of uncertainties; however, one important aspect is highly relevant to our discussion: some uncertainties are irreducible (namely, the aleatory uncertainty is an intrinsic attribute of a parameter and cannot be made smaller no matter how much we know) and others are reducible by accumulation of knowledge. The epistemic uncertainty can be decreased by more accurate measurements; the model completeness uncertainty is reduced once better, more complete and accurate models are developed.

One can loosely characterize the model parameter values as “unknown knowns” – due to the epistemic uncertainty; we know the values - but only so well, with a limited accuracy. On the other hand, the model completeness refers to what may be called “unknown unknowns”, i.e., the phenomena or effects that we do not know about and hence cannot reflect in the model. The inadequate model completeness may lead to what was occasionally called an “analytical failure mode” – a situation when a model fails to predict an important behavior which leads to a safety challenge.

When it comes to ways to accumulate knowledge and thus trim down the reducible components of uncertainty there are essentially only two options: R&D and OPEX. At this, when dealing with issues associated with phenomena occurring under accident conditions, it would be inappropriate to wait for operational experience data; experimental research supplemented by theoretical assimilation of information is the only feasible option.

Let us now consider a couple of specific and relatively recent examples, both dealing with the Large Break LOCA in CANDU reactors where a substantial R&D effort led to different outcomes. In the first case, the existing knowledge was enhanced and supported by the new information; in the second case, the new information necessitated revision of the earlier conclusions.

The first example refers to an extensive R&D effort to improve accuracy of thermal hydraulic modeling of large LOCA transients, in particular, the rate of coolant voiding, by reducing the epistemic uncertainty in modeling parameters and correlations.

> *Generic Action Item 00G01 "Channel Voiding During a Large LOCA" was initiated to deal with the issue of lack of experimental support for channel voiding rate predictions under conditions relevant to CANDU large LOCA. This included the issue of fuel sheath-to-coolant heat transfer rate and adequacy of steady-state CHF data for large LOCA voiding calculations. In addition, the effect of scaling on channel voiding rate needed to be addressed.*
>
> *The CANDU industry developed experimental techniques and conducted series of tests with void fraction measurements at RD-14M facility. Based on the new experimental data, relevant computer code validation exercises and the scaling assessment were completed. While residual questions related to validation and scaling methods remain, this activity confirmed the general adequacy of the computer codes used in the licensing safety analysis and allowed to better quantify uncertainty of models.*

The following is an example of a project aimed at reduction of completeness uncertainty by development, validation and application of more complete and accurate models. This R&D activity resulted in what could be termed a “discovery” (or “analytical model failure”) – i.e., realization that the previous licensing analysis was not in fact conservative.

> *Generic Action Item 99G02 "Replacement of Reactor Physics Computer Codes Used in Safety Analysis of CANDU Reactors" was opened to address several shortcomings in the reactor physics codes used at that time. The most important weaknesses were: lack of proper validation data for important phenomena and range of conditions, and a significant gap between the state of knowledge reflected in the codes and the current state of knowledge in the area resulting in inaccurate predictions of key parameters for accident conditions.*
>
> *In the course of computer code replacement activities, an analysis of a power pulse following a LLOCA with the new set of reactor physics codes resulted in the prediction of more severe consequences than those presented in earlier licensing submissions. To compensate the increase in the predicted power pulse some licensees had to implement more restrictive operating limits, such as flux tilt limit, moderator and coolant purity limits, and moderator poison load limit.*

Hence, the two above examples illustrate that the ongoing research effort while usually confirming the existing safety case of operating plants, may also bring realization that, in fact, uncertainties in earlier models were underestimated.

5. Balancing conservatisms and evaluations of risk

Assuming that the continuing research will result in increased knowledge and thus reduction of uncertainties associated with evaluations of safety, is it reasonable to expect that the conservatism built into design or safety analysis of a nuclear plant could be reduced as a consequence?

Indeed, the effort over years has led and continues to lead to the accumulation of data, theoretical understanding, and engineering models of ever-increasing complexity. At the same time, the computing hardware offers previously unattainable capabilities for numerical modeling.

It can be (and has been) argued that, in the drive for absolute safety while lacking wholesome capability to quantitative measure the achieved safety, the layers of safety measures have been added on other levels. For example, conservative estimate of safety challenges would be complemented by requirement of safety margins for a safety barrier, and then by the requirement of multiple consecutive barriers, and all this for the "worst case" scenario. The control or appreciation of the actual safety is thus not available.

We also acknowledge that the risk evaluation methods have matured and now offer, at least in principle, a systematic (even if not necessarily accurate) assessment of various threats and their costs to the society.

This proposes that conservatisms previously built into the design and analysis can be relaxed if and when shown to be excessive. The stipulation, of course, lies with the condition "if and when shown to be excessive" – this demonstration would be expected to be quite compelling. Here is why:

- Relaxation of rules in a given specific case must still maintain the overall safety levels. Moreover, the society expects ever-increasing protection from technological risks;

- It is expected that there would be clear economic benefit to the society from any change in the rules in a less conservative direction: the benefits of increased productivity should clearly outweigh the cost of maintaining conservatisms, with the price of transition included in consideration;

- Usually the research effort and therefore the accumulation of knowledge is focused on the areas where the safety margins are known or suspected to be small – in such cases, the benefit of increasing knowledge is in avoiding the need for further constraints rather than from the relaxation of existing ones;

- The complexity of analysis methods is growing exponentially – along with the effort required to build, validate, review and eventually approve new methods and their results.

Regardless of the constraints listed above, relaxations of certain safety restrictions have occurred, for example, in the following cases:

- power uprates in LWR practice that involve a combination of plant design changes as well as application of more advanced, less conservative safety analysis methods, such as Best Estimate plus Uncertainty LOCA methodology;

- in a similar vein, a Canadian licensee applied, and received approval, for a certain operational relaxation in the permitted power holds (power increase rates after restart) while using the BEAU methods in analysis of consequences of a Large Break LOCA.

While it is fully conceivable that conservatisms in specific analyses could be relaxed given the adequate support, the overall regulatory philosophy is believed to be balanced and justified. Following a period of un-eventful operation, comes a discovery or an operational event that confirms that unexpected may occur and could lead to unacceptable consequences were it not for the precautionary measures implemented in design. Occasionally, the precautionary measures prove to be insufficient. One example is undoubtedly fresh in our minds – the Fukushima Daiichi accident following the major earthquake and tsunami.

6. Specific examples

Below are two CANDU-specific "discoveries" in the field of thermalhydraulics, illustrating past "unknown unknowns" and the actions taken to address those:

- Bruce flow reversal and reactivity insertion

In 1993 it was realized that the positive reactivity insertion due to fuel string relocation reactivity was not accounted for in CANDU reactors with fueling against flow. In some events, this relocation resulted in a significant positive insertion of reactivity**.** Prompt criticality issue arose and lack of information related to fuel response under severe power pulse conditions had to be acknowledged. Remedial actions were quickly implemented by the affected licensees including operation at reduced power. Power increases were later granted based on new analysis and changes in the field such as core conversion involving changing the direction of re-fuelling.

The recognition of the reactivity effect associated with coherent and rapid relocation of all fuel bundle strings in the channels of the affected pass of a core during a LOCA had a rather profound impact on safety analysis. For reactor designs such as at Bruce and Darlington where fuelling was against the flow (i.e. new fuel bundles are introduced at the outlet end of fuel channels) the reactivity addition was positive and occurred shortly after the break is initiated. The rapid positive reactivity insertion that would occur before shutdown was initiated, compounded by the positive coolant void reactivity exacerbated the magnitude of the power pulse.

Additionally, the magnitude of reactivity insertion is dependent upon the pre-existing gap between the upstream end of the fuel string and the inlet shield plug - the gap being larger for older reactors due to uncompensated axial creep of the pressure tubes. The reactors most affected by this reactivity effect were those at Bruce A&B and Ontario Hydro voluntarily derated all the units to 60% FP until compensating measures could be established to offset the effect of the additional positive reactivity insertion. Design change measures included reversing the direction of fuelling in the Bruce A reactors and introduction of long fuel bundles in Bruce B and Darlington reactors as a means of fuel string/shield plug gap management. A significant safety analysis effort was initiated both to support the design modifications and to establish restrictions on the operating envelope that would allow the power level to be increased. Operating limits on allowable flux tilts were reduced significantly, as were limits on moderator and coolant isotopic purity and limits on moderator poison concentration. The latter restrictions were aimed at compensating for the fuel string relocation reactivity by reducing the magnitude of the coolant void reactivity feedback.

Inadvertently, a new challenge to fuel channel integrity was introduced with restrictions on the gap between the fuel string and the inlet shield plug. Relative thermal expansion of the overheated fuel string and pressure tube could result in a reduction of the gap and the possibility of constrained expansion if the fuel string expanded sufficiently to contact the shield plug. This resulted in an additional safety evaluation criterion, avoidance of constrained relative fuel string axial expansion, being introduced into the analysis.

- ***Darlington acoustic pulsation***

In 1990, Darlington Unit 2 experienced a fuel damage event, in which a bundle was extensively damaged during the attempted refuelling operation. The centre elements of a downstream bundle had broken loose, and had interfered with normal refuelling operations. The bundle was further damaged during the attempted refuelling.

Inspections of other outlet bundles in Darlington fuel bays revealed the presence of end plate cracks in multiple bundles. The post irradiation examination allowed concluding that the end plate cracks were the result of high cycle/low amplitude fatigue. Subsequent investigations demonstrated that the five vane impellers of the primary circuit pumps introduced pressure pulsations which were acoustically amplified within certain channels. The pulsation frequency of 150 Hz coincided with the resonant frequency of the inner seven fuel elements of the 37 element bundle. With fuel column latch support, which is unique to the Darlington and Bruce reactors, the non-outer fuel elements are unrestrained and free to vibrate in an axial direction. Axial vibration at the resonant frequency led to end cap cracking.

To eliminate the acoustic amplification of pressure pulsations in the fuel channels and to decouple the axial resonant response of the fuel, five vane pump impellers were replaced with seven vane impellers. This change shifted the pressure pulsation frequency from 150 to 210 Hz, which eliminated the end plate cracking problem at the Darlington reactor.

Following this incident it became clear that a better knowledge of the nuclear reactor acoustics was required to enable the designer, at least in principle, to address the problem of acoustic excitation. However, given the complexity of the primary heat transport (PHT) system geometry and uncertainty in thermalhydraulic conditions, the accurate prediction of its acoustic characteristics remains an extremely complex multi-disciplinary task. Testing of the PHTS and its components remains to be an important activity in confirmation of the system's acoustic performance.

7. Conclusions

Nuclear power technology has matured over a number of decades to the point where our understanding of the technology under a wide variety of circumstances is quite high. Despite this high degree of maturity, discoveries of new challenges occasionally surface. These may arise from either unusual or unexpected operational conditions or new experimental findings from ongoing research. With the early realization that such discoveries could occur, a conscious effort was made to take precautions against their negative impacts. Principles such as defence-in-depth, designing for high reliability, incorporation of robust safety margins and use of justified conservatisms are key examples of established practices that are embedded in national regulatory regimes of most, if not all countries with nuclear programs. Because of these provisions the safety cases of the current generation of reactors proved to be quite resilient to discoveries of earlier unrecognized challenges. Nevertheless, the implemented and evaluated safety provisions assure safety against known threats or challenges; this assurance is not necessarily there if a new challenge arises. Constant vigilance is necessary to avoid complacency and both the industry and the regulator should maintain adequate provisions to deal with "unknown unknowns".