31st Conference of the Canadian Nuclear Society (CNS)
Montréal, Québec
May 24-27, 2010

Safety analysis: its role and current trends

Alexandre Viktorov
Canadian Nuclear Safety Commission (CNSC)
Ottawa, Ontario, Canada

Abstract

Safety analysis is one of the components of the overall safety assessment required to demonstrate that a proposed nuclear power plant, once constructed, would operate safely, without posing unreasonable risks to the public, workers and the environment. It is also one of the so-called safety programs utilized by the CNSC in the on-going evaluations of safety performance of the operating plants. This presentation will explore why, after decades of safe nuclear power plant operation, the safety analysis remains to be an area of significant regulatory attention, both in general terms as well as from the Canadian perspective. With regard to the latter, the paper will touch upon specifics and evolution of the Canadian regulatory framework and some of the recent "discovery issues". The current trends, such as introductions of novel complex methods, ever-increasing attention to consideration of uncertainties, and prioritization based on safety significance will also be explored. Finally, this presentation will venture to consider potential future developments and expectations that may shape the safety analyses for nuclear power plants in the future.

1. Concepts of Safety Assessment, Safety Areas and Programs

Safety analysis is only one of several safety assessment activities

Safety assessment, as promulgated by the IAEA [1], is a comprehensive study to demonstrate that a nuclear facility would operate safely, without posing unreasonable risks to the public, workers and the environment. Safety assessment is conducted as a required pre-condition to obtaining a licence or approval for design or operational changes; it may also be conducted at regular intervals during the operating life of the facility or in response to certain circumstances, such as discovery of a major deficiency in the existing safety assessment.

For pragmatic reasons, the overall safety assessment is divided into several safety areas, mostly according to the disciplines involved. Table 1 below lists all Safety Areas used by the CNSC until recently while Table 2 presents the list of safety areas that was revised by CNSC staff taking into account the accumulated experience (one of the reasons for revision was the intent to expand its applicability beyond nuclear power plants). It is apparent that the overall safety assessment of a facility can be subdivided in any number of ways depending on the complexity of the facility and the level of desired regulatory scrutiny; in any case Safety Analysis will remain to be one of key safety areas.

Table 1 - Safety Areas used by the CNSC until 2010

Safety Area	Sub-Areas
1. OPERATING PERFORMANCE	Organization and Plant Management
	Operations
	Occupational Health and Safety (Non-radiological)
2. PERFORMANCE ASSURANCE	Quality Management
	Human Factors
	Training, Examination, and Certification
3. DESIGN AND ANALYSIS	Safety Analysis
	Safety Issues
	Design
4. EQUIPMENT FITNESS FOR SERVICE	Maintenance
	Structural Integrity
	Reliability
	Equipment Qualification
5. EMERGENCY PREPAREDNESS	
6. ENVIRONMENTAL PROTECTION	
7. RADIATION PROTECTION	
8. SITE SECURITY	
9. SAFEGUARDS	

Table 2 - Revised set of Safety Areas

Safety and Control Areas	Sub-Areas or Programs (examples)
Management System	• Management System • Monitoring and Review of Safety Management Performance • Management of Safety Issues (including R & D Programs) • …
Human Performance Management	• Personnel Training • Personnel Examination and Certification • …
Operating Performance	• Conduct of licensed activity • Operating Experience (OPEX) • …
Safety Analysis	• Deterministic Safety Analysis • Probabilistic Safety Analysis • Hazard Analysis • Safe Operating Envelope • Robustness Analysis • Criticality Safety
Physical Design	• System Classification • Facility Safety Systems • Reactor Control Systems • Configuration Management • …
Fitness for Service	• Equipment Fitness for Service/Equipment Performance (e.g. System Health Report) • Reliability • Ageing Management • …
Radiation Protection	• Application of ALARA • Dosimetry Services • …
Conventional Health and Safety	• Compliance with the applicable Labour Code • …
Environmental Protection	• Effluent and Emissions Control • …
Emergency Preparedness	• Nuclear Emergency Management • …
Waste Management	• Waste minimization, segregation and characterization • …

Safety and Control Areas	Sub-Areas or Programs (examples)
Security	• Facility Security • …
Safeguards	
Packaging and Transport	

Just as Safety Analysis is part of a more generic activity, it in turn is subdivided into several sub-elements.

Note, that while the concept of safety assessment would apply to any nuclear facility or activity, it is the safety analysis for nuclear power plants that will be the focus of discussions below. This presentation will explore why, after decades of safe nuclear power plant operation, the safety analysis program remains to be an area of significant regulatory attention, both in general terms as well as from the specific Canadian perspective.

2. Definition and Objective of Safety Analysis

Safety analysis aims to demonstrate plant's safety in case of malfunctions and errors

In general sense, safety analysis is an evaluation of potential risks to the public, workers and environment associated with the facility. Expanding on this basic definition, we will call "safety analysis" a process which:

- aims to quantify the attributes of various hazards, namely their probability and impacts or consequences;
- considers all possible plant states from normal operation up to significant and multiple equipment failures or operator errors;
- uses well structured formal methods;
- is based on up-to-date knowledge gained through experience or scientific research;
- in the end, allows to compare with high confidence the potential risks associated with the facility against the regulatory requirements.

Safety analysis deals with hypothetical events deemed likely or at least possible to occur at the facility; the focus of the probabilistic analysis is on the quantification of probabilities of accidents, whereas the deterministic analysis predicts the consequences of a postulated accident.

Naturally, for a well designed plant, it is expected that the safety analysis will demonstrate that for all credible events, such as malfunction of equipment, operator errors or common cause events, the risks to workers, public and the environment are within the allowed limits.

Note that the current safety analysis methods cannot reliably capture effects of how well the plant is operated and maintained, or how well the operators are trained.

3. Safety Analysis program

Safety analyses are performed under governance of an established program

Definitely, a programmatic approach to performing safety analysis is not a novel notion, however it has only firmed up as a principle probably in the last decade, and perhaps it is still in the process of being accepted as a customary practice. It is indisputable though that the safety analysis is not performed just once in the lifetime of a plant but is rather an ongoing process set up to react to the various demands. Experience shows that such demands are much more likely to arise for a large sophisticated facility such as a nuclear power plant, rather than for a small research reactor. From the modern project management it follows that efficiency is to be gained through development of a programmatic approach to conduct of similar projects.

According to the dictionary definition, a program is a process of managing of several related projects, with the intention of improving the overall efficiency. A safety analysis program sets forth a coherent framework of requirements, practices and responsibilities related to performing safety analyses. As the regulator, the CNSC expects all licensees to have firmly established safety analysis programs as part of their overall safety management system; regulatory evaluation of licensee's performance in "Safety Analysis" area (Tables 1&2) without doubts includes consideration of the programmatic aspects.

Key attributes of a Safety Analysis program sought by the CNSC can be summarized as follows:

- Alignment: The program must support higher level organizational goals and objectives.
- Governance: The program must include a set of metrics to indicate the health and progress of the program in the vital areas.
- Management: Roles and accountability of management, participants, stakeholders and suppliers are defined.
- Integration: The program performance is optimized through integration of program components.
- Resources: Costs of administering the program are tracked and assessed. Allocation of resources promotes success of the program.
- Planning: Working plans tying together the priorities, projects, resources, timescales, monitoring and control are developed.
- Assurance: The program is reviewed, verified and validated, ensuring adherence to applicable standards and goals.
- Improvement: Performance is continuously assessed; new capabilities are researched and developed; and new knowledge is systemically applied to the program.

From the regulatory perspective, compliance with the safety analysis program is an essential element of the overall safety performance.

4. Safety Analysis regulatory framework

Regulatory framework for safety analysis is evolving

While safety analyses were performed for the very first nuclear power plants, the expectations for safety analysis as well as the capabilities to perform it have greatly advanced since then. It is relatively easy to distinguish several major phases in the Canadian regulatory framework applied to the safety analysis; notable differences among those are examined below.

Table 3 - Safety Analysis regulatory frameworks

	Siting Guide, AECB-1059, R-10	**C-6, R-7, R-8, R-8**	**RD-310, RD-337**
Analysed events	Single (process) failure (1 in 3 years) Dual (process + safety system) failure (1 in 3000 y)	Prescribed list of events binned into five classes	Applicant to identify events using a systematic process. Classify as AOO, DBA or BDBA based on probability
Acceptance criteria	Dose limits to the public. Minimizing damage to fuel. Minimizing escape of fission products from plant.	Dose limits to the public. Effectiveness criteria for special safety systems.	Dose limits to the public. General qualitative acceptance criteria and applicant-defined quantitative criteria.
Analysis assumptions	Unavailability of special safety systems. Specific weather category and model for calculation of public doses	Unavailability of special safety systems. Rules for availability of off-site power. Double guillotine pipe failure. Single-failure criterion.	Single failure criterion. Consider consequential failures. Consider equipment being out of service
Analysis models / computer codes	No guidance	Conservative predictions. All important phenomena to be considered. Justified simplifications. Verification by experimental evidence.	Computer codes to comply with CSA 286.7
Conservatism	No guidance	Input parameters to ensure conservative predictions	Conservatism to off-set uncertainties

	Siting Guide, AECB-1059, R-10	**C-6, R-7, R-8, R-8**	**RD-310, RD-337**
Treatment of uncertainties	No guidance	Use of conservative correlations Use of limiting assumptions where models are not suitable	Analysis method to include accounting for uncertainties
QA / analysis review	Follow the best applicable codes, standards or practices	Analysis rules to be approved by the AECB, including use of mathematical models	Systematic analysis method. Review of analysis results. Comprehensive QA program.

On the other hand, one can distinguish several major stages in the development of the analysis methods [2]. Such development was necessitated by very specific needs, more often than not related to the Large Break Loss of Coolant Accident analysis.

For example, “limit-consequence” methodology applied analysis assumptions to assuredly envelope the possible reactor conditions and event characteristics in such a way that maximized the consequences. The driver for using this approach was to circumvent the gaps in supporting experimental data and models. Thus, limiting assumptions were made with regards to the phenomena and not necessarily systematically when considering the reactor operating parameters. The idea was that if a very conservative analysis showed acceptable results then the relatively accurate knowledge of accident phenomena was not crucial to gain regulatory acceptance.

The “limit consequence” was convenient as a relatively simple approach and perhaps the only option when the modelling capabilities were not allowing more accurate representation of all important phenomena. It also predicted results that, in some cases, were not acceptable. The ensuing advancement of the knowledge base and modeling tools permitted development of an approach that is still widely in use - the Limit of Operating Envelope (LOE) method. The LOE relies on the use of best estimate codes and assumes bounding operating parameters such that the safe plant operation can be demonstrated. Analysis values of key operating parameters are set at their operating limits plus uncertainty allowance; this makes the analyzed plant state to be highly unlikely but still possible. It is assumed (and recently has been confirmed through the BEAU analysis at least for one case) that the LOE method produces conservative results.

Best Estimate Analysis with Uncertainties (BEAU) method [3] arose from the need to better quantify safety margins for events where the LOE analyses showed small, and diminishing, margins. BEAU represents a more systematic method for accounting for various sources of uncertainties and generating results with desired level of probability and confidence. This is achieved through explicit consideration of uncertainties in key analysis parameters and application of statistical techniques to propagate these uncertainties up to the output parameters. While CNSC staff concluded that the recent pilot BEAU applications were not fully and adequately supported, we also find that this method offers numerous useful insights and has

undeniable merits. Its future use and success will depend on resolution of few key challenges, primarily, the ability to quantify the modelling uncertainties.

5. Will Safety Analysis ever be done?

Safety analysis is an on-going activity

Let explore the statement made in the preceding section that the analysis is an ongoing process in response to various demands. What kind of "demands" could that be? Will they always be there? These can be grouped into the following four categories:

Table 4 - Demands for Safety Analysis

Analysis Demand Items	Examples	Summary Likelihood
1.Changes in the design of systems	- new fuel design - units in safe storage	Moderate (about once per year)
2.Changes in operating conditions or limits	- ageing effects - power penalty recovery - parallel parking of FM under a unit in a multi-unit station	Moderate (about once per year)
3."Discovery[1]" issues	- neutron flux tilts not accounted for in analyses - fuel relocation reactivity - increasing VREA - physics codes non-conservatism - CHF for 28-element bundle	Relatively rare (about once in 5 years) - negative impact on the licensee
4.Changes in regulatory requirements	- code validation requirement (G-149/GAI / CSA286.7) - transition to RD-310?	Rare

The first two reasons for performing a new analysis are mostly in response to operational needs of a licensee, and rarely in response to findings that the current plant operation may not be meeting regulatory requirements. It is unusual when the plant design or operational conditions would be found such that the safety is seriously questioned; such cases would be treated as “discovery” issues.

[1] Discovery issue – in the context of safety analysis, is a previously unknown or underestimated issue, which has the potential of significantly reducing margins demonstrated in the facility’s Safety Analysis Report.

At the same time, “discovery” issues have been occurring regularly in the Canadian practice. In such cases changes in either design or operating conditions may be necessary, in addition to a revised analysis. One can speculate that the relatively regular occurrence of "discoveries" can be explained, at least partially, by the relatively scarce CANDU-prototypic experimental data to develop and validate analytical models or fully test performance of all systems up front.

Will the above drivers fully disappear in the near future? There is no reason to think so - the plant operator may always wish to improve plant operations by modifying design or operating conditions. On the other hand, occurrence of "discoveries" can not be controlled or predicted but these can never be ruled out completely. It makes sense, though, to think that the likelihood of the need to redo safety analyses will decrease.

6. Recent developments

Several factors are in play to change current expectations for safety analysis

6.1 New regulatory expectations

We saw in the recent years a significant evolution of the expectation and practices in the area of safety analyses. The following comes to mind:

- introduction of new regulatory documents (RD-310 for deterministic SA)
  - increasing role of accounting for uncertainties;
  - understanding of conservatisms;
  - justification of acceptance criteria
  - quantification of safety margins
  - accounting for ageing effects;
  - control of methodologies;
- standardization of computer codes though the IST program with more stringent requirements for verification and validation of codes (CSA 286.7)
  - formal code validation
  - quantification of modelling uncertainties
- development of new analytical methodologies or formalization of old ones
  - Formalization of the LOE method
  - Development of the BEAU method and guidelines
  - Extreme Value Statistics (EVS) method
- wider use of the international benchmarking and best practices, including recommendations from IAEA

6.2 PSR/ISR

Periodic Safety Review (or its current Canadian variety, Integrated Safety Review) introduces a formal process of a periodic comparison of selected safety factors (safety analysis being one of them) against modern standards and best practices. Any gaps identified are addressed using a formal process which assesses the safety significance of the gap and considers costs associated with its resolution. This allows a conscious decision-making with regards to those safety analysis shortcomings that are not sufficiently safety significant and can be allowed to exist; at the same time the more important issues would be addressed on a priority basis.

6.3 New build

The planned new nuclear build necessitated a fresh look at the expectations for safety analysis (which are now reflected in the recently issued regulatory documents). Facing potential introduction of non-CANDU technology, an effort was undertaken to develop technology-neutral regulatory requirements and expectations. At the same time, to help CNSC staff as well as to assist potential applicants who may not be familiar with the established Canadian practices, detailed review guidance is being prepared.

This includes expectations to the contents and structure of Safety Analysis Reports. Two alternatives emerged – one following the US NRC Standard Review Plan [4], and the other one using the table of contents as given by the IAEA [5]. Both of these alternative include under the title of Safety Analysis Report much more than has been the practice for the currently operating plants (for example, the PSA would be a part of the Safety Analysis Report).

7. What s in the future?

Twenty years from now safety analysis may look quite different

If we take some of the recent trends in safety analysis and extrapolate them, say, 10-20 years in the future, what will we get? To help us answering the question, let put together a list of the key factors that are "shaping" these trends:

- accumulation of knowledge and data to close outstanding knowledge gaps
- fast development of computational and data storage capabilities
- expectation of continuously improving safety
- increased use of risk informed prioritization
- expectation of improved plant performance
- tighter cost controls
- increasing harmonization of national regulatory approaches.

Clearly, these factors do not pull in the same direction, but with some imagination the following seems if not likely then at least technically possible:

a) Digitalized plant design - all design parameters maintained up to date electronically) and available for multiple uses, including safety analysis. Any changes in SSC would be immediately indicated for assessment for their impact on safety analysis.

b) Fully coupled plant models - physics, thermal-hydraulics, fuel and channel behaviour, structural mechanics, etc.

c) Single input file for all safety analysis.

d) Advanced complex models - multi-phase CFD (TH), Monte-Carlo (physics), finite element models in fuel and channel deformation, etc.

e) Detailed consideration of uncertainties – aleatory and epistemic, operational and modelling.

f) Tuning of the conservatism concept to suit the analysis objectives and type of the event analyzed (AOO, DBA, BDBA).

g) Wider use of statistical techniques.

h) Intrinsic links to PSA - probability based analysis rules/assumptions.

i) Maturity of prioritization techniques (RIDM, CBA, etc) to provide better correlation of analysis priorities with safety or operational benefits.

j) Living deterministic safety analysis - i.e., analyses that are updated in (near-) real time to follow the plant configuration and operating parameters. This can be based on a combination of detailed (pre-existing) calculations and interpolation techniques to make the updating fast. This will allow monitoring, in the real-time mode, changes in potential consequences of postulated events as function of the actual plant state. This may also offer further opportunities for reductions of built-in conservatism of the modern safety analysis.

It remains to be seen whether any of the above will come about. One thing for sure – safety analysis will continue to evolve.

8. References

[1] IAEA Safety Standards GSR Part 4, Safety Assessment for Facilities and Activities, 2009.

[2] J. Luxat, “Safety Analysis Technology: Evolution, Revolution and the Drive to Re-Establish Margins”, Presentation to CNS seminar, September 13, 2000.

[3] Guidelines for Application of the Best Estimate Analysis and Uncertainty (BEAU) Methodology to Licensing Analysis. COG-6-9012, Rev 1., April 2008.

[4] US NRC NUREG-800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants.

[5] IAEA Safety Guide GS-G-4.1, Format and Content of the Safety Analysis Report for Nuclear Power Plants.