Application of Probabilistic Safety Goals to Regulation of Nuclear Power Plants in Canada

G. Rzentkowski, Y. Akl, S. Yalaoui
Canadian Nuclear Safety Commission
P.O. Box 1046, Station B
Ottawa, Ontario, Canada K1P 5S9

Abstract

In the Canadian nuclear regulatory framework, Safety Goals are formulated in addition to the deterministic design requirements and the dose acceptance criteria so that risk to the public that originates from accidents outside the design basis is considered. In principle, application of the Safety Goals ensures that the likelihood of accidents with serious radiological consequences is extremely low, and the potential radiological consequences from severe accidents are limited as far as practicable. Effectively, the Safety Goals extend the plant design envelope to include not only the capabilities of the plant to successfully cope with various plant states, but also practical measures to halt the progression of severe accidents.

This paper describes the general approach to the development of the Safety Goals and their application to the existing nuclear power plants in Canada. This general approach is consistent with the currently accepted international practice and Canadian regulatory experience. The results of probabilistic safety assessments indicate that the Safety Goals meet or exceed international safety objectives due to effective implementation of the defence-in-depth principle in the reactor design and plant operation. At the same time, the application of the Safety Goals reveal that practicable measures exist to further enhance the overall level of reactor safety by focusing on severe accident prevention and mitigation. These measures are being currently implemented through refurbishment projects and feedback on operating experience.

1. Background

The CNSC has been reviewing the regulatory framework for licensing new Nuclear Power Plants (NPPs) in response to the interest in a nuclear energy option in Canada, [1]. The intention underlying this work is to update the licensing basis for future power reactors; namely, a set of comprehensive requirements for design, siting, construction and operation of NPPs which are risk-informed and closely aligned with accepted international practices.

The first step in updating the licensing basis was the revision of the requirements for the design of nuclear power reactors, [2,3]. The IAEA Safety Standard NS-R-1[1], [4], was selected as the underlying template for the development of these requirements which, to a large extent, are technology neutral. The new requirements are documented in the regulatory document RD-337, [5]. Since the Canadian regulatory framework was largely constrained to the design basis accidents, the new design requirements place particular emphasis on severe accident prevention and mitigation, [6]. Consequently, the design envelope[2] for new nuclear power plants has been

[1] IAEA NS-R-1 is now superseded and replaced by IAEA Specific Safety Requirements No SSR-2/1
[2] A plant design envelope comprises design capabilities for all credible plant states considered in the design, including normal operating, AOO, DBA, and BDBA states.

extended to include not only the capabilities of the plant to successfully cope with various plant states -- ranging from normal operation, Anticipated Operational Occurrences (AOOs)[3] and Design Basis Accidents (DBAs)[4] -- but also complementary, practical measures to halt the progression of Beyond Design Basis Accidents (BDBAs)[5].

The new design requirements, [5], include clear Safety Goals that an NPP design must meet to minimize any significant additional risk to the public in comparison with other risks to which the public is normally exposed. Consistent with international practice, [4], Safety Goals are formulated in addition to the deterministic design requirements and the dose acceptance criteria so that risk to the public that originates from accidents outside the design basis is considered. Specifically, the qualitative health objective states that individuals should bear no significant additional risk to life and health as a consequence of the operation of an NPP. Furthermore, the associated societal risks to life and health should be comparable or less than the risks of competing technologies. This is expressed in terms of the risk of a fatality caused by the operation of an NPP being a small percentage (typically less than 1%) of the risk posed by other industrial activities and societal risks, as recommended by US Nuclear Regulatory Commission, [15]. The quantitative health objectives are not explicitly stated as part of the new design requirements.

This paper describes the general approach to the development of the Safety Goals and their application to existing NPPs Canada. The results of the Probabilistic Safety Assessment (PSA) indicate that the Safety Goals meet or exceed international safety objectives due to effective implementation of the defence-in-depth principle in the CANDU design, although the potential consequences from severe accidents were initially only implicitly addressed by considering dual failures events which, as reflected in the document known as the Siting Guide, [7], involve a process system failure coinciding with a safety system failure. As a result, unlikely combinations of events, such as a Loss of Coolant Accident with a consequent Loss of Emergency Coolant Injection, were included in the plant design. It should be noted here that, besides specifying the radiological dose limits for dual failure events, the Siting Guide also suggests to minimize the likelihood of dual failures by setting limits on the frequency of the initiating single failure event and the probability of failure on demand of protective devices.

An application of the dual-failure approach has undoubtedly led to a robust reactor design and assurance of high reliability of reactor process and safety systems. The Safety Goals, however, through the application of PSA allow examination of severe accidents in a more systematic manner to clearly demonstrate that the residual risk associated with multiple failures of protective barriers is minimized to the extent practicable. Furthermore, they allow identification of practical safety improvements for severe accident prevention and mitigation to further improve safety of operating NPPs in Canada. More specifically, the risk perspective gained from PSA is used to evaluate and optimize the overall defence-in-depth strategy by identifying the

[3] An operational process that deviates from normal operation without exceeding safety limits to result in an accident condition.
[4] Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.
[5] Accident conditions less frequent and more severe than DBAs that include severe accidents, resulting from multiple failures of protective barriers that could potentially lead to severe degradation of the reactor core.

design basis challenges to physical barriers and by judging their acceptability based on the derived acceptance criteria. A high level of independence of the different levels of protection is a prerequisite for avoiding cascading failure propagation from higher to lower level of defence-in-depth. Incorporation of risk insights, supported by a comprehensive plant specific PSA, is thus essential in balancing strategies of accident prevention and mitigation; that is, higher frequency initiating events and event sequences rely more on prevention, whereas lower frequency initiating events and event sequences rely more on mitigation. In principle, implementation of the Safety Goals ensures that the likelihood of accidents with serious radiological consequences is extremely low, and the potential radiological consequences from severe accidents are limited as far as practicable.

2. Safety Goals

There are two fundamental health effects on the public; one relating to early fatalities and the other relating to late or delayed fatalities. Early fatalities are linked to accident rates (e.g. industrial, traffic, etc.) while late fatalities are linked to cancer rates. The actual numerical safety goal limits, relating to the prevention and mitigation of accidents that are typically used in the nuclear power industry, are conservative surrogates to these health effects to simplify their calculation. They are the Severe Core Damage Frequency (SCDF) goal, and the Large Release Frequency (LRF) goal, as shown in Table 1 below, [9].

The SCDF goal is a defence-in-depth measure designed to limit reliance on the containment system (prevention). The frequency of accidents that could lead to severe core damage is very low, i.e., less than once every hundred thousand years, and it is widely accepted in the international nuclear community.

The LRF goal refers to the frequency of an off-site release that would result in the need for long-term, or even permanent, evacuation of the surrounding population as a result of extensive ground contamination. A numerical value of once every million years for the frequency of such events, as shown in Table 1 below, is generally accepted in the international nuclear community. It is also accepted that by setting the release limit to $1 \times 10^{+14}$ Bq of the Cesium isotopes Cs-137, long-term ground contamination of large areas could be avoided [8]. The release limit is equivalent to 0,1% of the inventory of the Cesium isotopes Cs-134 and Cs-137 in a core of a 1800 MW reactor, excluding noble gases. The limit of $1 \times 10^{+14}$ Bq of Cs-137 release also corresponds to 1% of the Chernobyl accident radioactive release. Although this frequency limit is generally accepted internationally, its application is inconsistent; countries with large international programs define the large release frequency limit per reactor year (e.g., France, Japan, Canada, USA) and countries with small nuclear programs define it per year (e.g., Finland, Switzerland, Sweden). The latter approach is generally more restrictive.

In CANDU reactors, some accident scenarios may result in limited core damage, leading to small releases but which can result in severe disruption of public life. These accidents require emergency measures such as sheltering or short term evacuation of an area around the plant. This concern is covered by the Small Release Frequency (SRF) goal.

CNSC staff decided that the small release frequency should be identical to the core damage frequency, as shown in Table 1 below, as both events are characterized with the release that would likely trigger evacuation. The intervention level, as per Health Canada [10], states that evacuation is recommended if the action will avert a dose of at least 50 mSv over a period of up to 7 days. Setting the small release goal to $1x10^{+15}$ Bq of the Iodine I-131 would lead to meeting the (50 mSv) threshold in a 2 to 3 kilometres zone around a CANDU plant, and avoidance of public evacuation.

Table 1: Safety Goals in Canadian Regulatory Framework [5]

Safety Goal	Rational	Numerical Objective [Sum of frequencies of all event sequences]
SCDF	**Accident prevention**	**Core degradation frequency is less than 1×10^{-5}**
SRF	**Release that would trigger evacuation**	**Release frequency of more than $1 \times 10^{+15}$ Bq of I-131 is less than 1×10^{-5}**
LRF	**Release that would trigger long term relocation**	**Release frequency of more than $1x10^{+14}$ Bq of Cs-137 is less than 1×10^{-6}**

3. Application of Safety Goals

The current regulatory processes ensure that nuclear facilities are designed, constructed, commissioned and operated so that individuals, the public and the environment are protected from radiological hazards.

The Safety Goals are not the primary means by which nuclear facilities are regulated. In general, they enable the CNSC to focus on the issues which can enhance the effectiveness of the regulatory process and ultimately lead to a safer nuclear industry and to provide an effective means of focusing all parties' attention on the most safety significant aspects of nuclear activities.

More specifically, the CNSC uses the Safety Goals as a clear statement of the desired level of safety which the regulatory process aims to deliver. The safety goals are also considered along with other key elements of the risk informed decision approach, [6], such as the defence-in-depth principle, the safety margin, and the regulatory requirements in order to make an informed decision.

3.1 Operating Nuclear Power Plants

For operating plants in Canada, the SCDF and LRF safety goals are used to estimate the likelihood of accidents which potentially may lead to serious radiological consequences. The likelihood of accident is expressed as a sum of frequencies of all events sequences, typically either internal or external, that can lead either to core degradation or a release to environment.

The limit of these frequencies should be no more than one order of magnitude higher, [8], than those for new power plants, [9], namely:

- SCDF less than 10^{-4} per reactor year
- LRF less than 10^{-5} per reactor year

All the licensees have identified the SCDF and LRF safety goals which for each site, except Gentilly-2 which ended its commercial operation in December 2012, are shown in Table 2. The Safety Goals are set as limits and targets. It can be seen that the target established for the Point Lepreau station is an order of magnitude lower than that for multi-unit stations. It reflects the safety objectives established for the refurbishment project and the long-term operation of the Point Lepreau station. As per the regulatory document RD-360, [11], an Integrated Safety Review (ISR) has to be performed in support of plant life extension to determine the extent to which the plant conforms to modern standards and practices, including the Safety Goals, and identify practicable safety improvements.

Table 2: Safety Goals for Canadian Nuclear Power Plants (mean values)

	Bruce Power		**OPG**		**Point Lepreau**	
Safety Goal [Reactor Year]	**Limit**	**Target**	**Limit**	**Target**	**Limit**	**Target**
SCDF	**1 x 10^{-4}**	**1 x 10^{-5}**	**1 x 10^{-4}**	**1 x 10^{-5}**	**1 x 10^{-4}**	**1 x 10^{-5}**
LRF	**1 x 10^{-5}**	**1 x 10^{-6}**	**1 x 10^{-5}**	**1 x 10^{-6}**	**1 x 10^{-5}**	**1 x 10^{-7}**

The main tool for demonstrating that the NPP design meets Safety Goals is PSA; Level 1 for the assessment of plant failures and responses of reactor systems (core damage frequency), and Level 2 for the assessment of containment response (large release frequency). The consequences to the public (doses) and to the environment are assessed using the Level 3 PSA. Consistently with the international practice, this level of assessment is not required by the CNSC.

All the licensees have already completed the Level 1 and Level 2 PSA for internal events in accordance with the regulatory document S-294, [12]. Table 3 shows that for all sites the results comply with the limits established for operating reactors. The PSA results, however, will be updated by the end of 2013 and do not include external events -- such as seismic, flooding and fire -- for which the licensees have recently developed the assessment methodologies. The assessments of external events will be completed for all sites by the end of 2014. It is important to realize that contribution from seismic or fire events may, in some cases, approach or even exceed that from internal events. Most dominant contributors could typically be either failures of offsite power or failure of various components of the reactor electrical distribution system.

Table 3: Safety Goals for Canadian Nuclear Power Plants - PSA Results (mean values)

	Bruce A	Bruce B	Darlington	Pickering A	Pickering B	Point Lepreau
SCDF	3.0×10^{-5}	2.5×10^{-5}	7.9×10^{-6}	3.6×10^{-5}	4.2×10^{-6}	8.6×10^{-6}
LRF	8.9×10^{-7}	6.2×10^{-8}	5.2×10^{-6}	5.0×10^{-8}	3.9×10^{-6}	6.5×10^{-8}

The Safety Goals presented in Table 3 indicate that in some instances, in particular Point Lepreau, the results clearly exceed the targets, reflecting safety benefits of the design improvements implemented during the refurbishment. It is thus expected that the Safety Goals for the Darlington and Bruce sites will further improve once all units have been refurbished even with the addition of external events.

The Safety Goals do not include safety benefits achieved recently through further design and operational measures aimed at preventing severe accidents and mitigating their consequences. These measures are being implemented at all Canadian NPP sites -- as a result of lessons learned from the natural disaster in Japan in March 2011 which led to nuclear accident at the Fukushima site -- to further reduce the likelihood of accidents which potentially may lead to serious radiological consequences.

3.2 Application to Multi-Unit Sites

As discussed, Safety Goals are defined in terms of events per reactor year. However, the effects of adjacent units at multi-unit stations are considered and accounted for when calculating Safety Goals for internal events sequences at the representative unit (generally, the lead unit). This means that the consequential accident sequences at the adjacent units are added up to calculate the sum of frequencies of all events sequences at the representative unit (as an example, the effects of a steam line break and feedwater line breaks in adjacent units are always included).

It thus follows that for certain internal events sequences the probability of an accident per reactor year, which could lead either to core degradation or a release to environment, would be higher at a multi-unit station in comparison to a single-unit station, assuming that there are no major differences in the design of reactors. For certain external events sequences, which may affect all units simultaneously, the probability of an accident per reactor at single and multi-unit stations would be the same whereas consequences at a multi-unit station would be more severe (consequences for the lead unit multiply by a number of units at a site) than those at a single-unit station.

It is important to note that in terms of events per site year, the probability of an accident for certain internal events sequences would approximately be the sum of the accident probabilities for each unit at a multi-unit site. Therefore, the licensees strive to meet the targets rather than the limits in identifying the areas of potential safety improvements and deciding on design upgrades (compare Table 2 and 3).

3.3 Environmental Assessment

As recommended in the IAEA safety standards NS-R-3, [13], an evaluation of the potential radiological impacts of normal discharges and accidental releases of radioactive material, including reasonable consideration of releases due to severe accidents, shall be performed with the use of site specific parameters as appropriate. The document also states that the radiological risk to the population associated with accident conditions, including those that could lead to emergency measures being taken, shall be acceptably low.

Following this international guidance, for the purpose of environmental assessment of any construction project at a reactor site, the CNSC staff decided to use the cut-off frequency which corresponds to the LRF for new builds. This requires a description of postulated accident sequences leading to radiological release that could occur with a frequency greater than 1×10^{-6} per year, considering as appropriate internal events, external events and human-induced event (including an explanation of how these events were identified, and any modeling that was performed). The selected cut-off frequency is one order of magnitude lower than the accepted large release frequency for the existing nuclear power plants and thus constitutes a reasonable consideration of releases due to severe accidents. The assessment is done per reactor year, taking due account of the effects of adjacent units at multi-unit stations, as explained in Section 3.2. This approach is also in line with the regulatory document RD-346 [14] which requires that site evaluation against the Safety Goals.

4. Summary and Conclusions

Safety Goals are formulated in addition to the deterministic design requirements and the dose acceptance criteria so that risk to the public that originates from accidents outside the design basis is considered. They are consistent with currently accepted international practice and Canadian regulatory experience.

Safety Goals enhance the overall level of reactor safety. In principle, Safety Goals ensure that the likelihood of accidents with serious radiological consequences is extremely low, and the potential radiological consequences from severe accidents are limited as far as practicable. Effectively, the application of the Safety Goals extends the plant design envelope to include not only the capabilities of the plant to successfully cope with various plant states, but also practical measures to halt the progression of severe accidents.

The Safety Goals calculated for all NPPs operating in Canada indicate that they meet or exceed international safety objectives due to effective implementation of the defence-in-depth principle in their design. Nevertheless, the calculated Safety Goals also demonstrate that through further design and operational measure, aimed at preventing severe accident and mitigating their consequences, the likelihood of accidents which potentially may lead to serious radiological consequences could be further improved. These measures are being implemented in the Canadian reactors as part of refurbishment activities, and as a result of lessons learned from events and accidents such as, for example, the natural disaster in Japan in March 2011 which led to nuclear accident at the Fukushima site.

5. References

[1] G. Rzentkowski, I. Grant, T. Viglasky, "Development of Licensing Basis for Future Power Reactors in Canada", Proceedings of the 26th Annual Canadian Nuclear Society Conference; June 2005.

[2] G. Rzentkowski, A. Banas, D. Miller, "An approach to the Development of Licensing Basis for New Power Plants in Canada", Proceedings of the 25th Annual Canadian Nuclear Society Conference, Toronto, Canada, June 2004.

[3] CNSC Pre-consultative Draft Document, "*Requirements for Design of Nuclear Power Plants*", March 2005.

[4] IAEA, "Safety of Nuclear Power Plants: Design Safety Requirements", Safety Standard Series No. NS-R-1, October 2000.

[5] CNSC, Regulatory Document RD-337: "Design of New Nuclear Power Plants", September 2008.

[6] G. Rzentkowski, V.Q. Tang, "A Risk-Informed Approach to the Development of Severe Accident Requirements", Proceedings of the 28th Annual Canadian Nuclear Society Conference; June 2007.

[7] G. C. Laurence, "Reactor Siting Criteria and Practice in Canada", AECB #1010, Presented at the American Nuclear Society National Topical meeting on Nuclear Reactor Power Siting, Los Angeles, February 1965.

[8] Jan-Erik Holmberg, VTT, Finland; Michael Knochenhauer, Relcon Scandpower AB, Sweden, NKS Probabilistic Safety Goals; Phase 1- Status and Experiences in Sweden and Finland, March 2007.

[9] IAEA, INSAG-12; "Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1", INSAG-12, Vienna, 1999

[10] Health Canada http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/guide-03/index_e.html

[11] CNSC, Regulatory Document RD-360: "Life extension of Nuclear Power Plants", February 2008.

[12] CNSC, Regulatory Document S-294: "Probabilistic Safety Assessment (PSA) for Nuclear Power Plants", April 2005.

[13] IAEA, "Safety of Nuclear Power Plants: Site evaluation for Nuclear Installations". Safety Standard Series No. NS-R-3, Vienna, 2003.

[14] CNSC, Regulatory Document RD-346: "Site evaluation for Nuclear Installations", November 2008.

[15] US-NRC, SECY-01-0009, "Modified Reactor Safety Goal Policy Statement".

e-Doc 4098021