Introduction to the

2015 Darlington NGS Probabilistic Safety Assessment

Carlos Lorencez and Robin Manley

Ontario Power Generation

August 2015

Introduction to the 2015 Darlington NGS Probabilistic Safety Assessment

Objective

In a number of Licensing Hearings over the past years, it has been clear that a significant amount of confusion exists about what is called a Probabilistic Safety Assessment (PSA). This article provides the necessary basic information needed to understand the preparation, interpretation and application of PSAs in the Nuclear Industry and, based on this information, provides an overview of 2015 Darlington NGS Probabilistic Safety Assessment (DARA) update. It is assumed that the reader has a basic understanding of nuclear power plant design. If not, it may be useful for the reader to first read some material on nuclear power plants available on the CNSC website or on OPG.com.

As part of Darlington NGS relicensing application, Ontario Power Generation (OPG) has prepared a detailed and technical assessment for Darlington NGS. A summary report of all PSA elements, NK38-REP-03611-10072, *Darlington NGS Probabilistic Safety Assessment Summary Report*, is posted on OPG's website.

Safety Analysis

In the early days of the civil nuclear power program, prior to the development of the PSAs, the nuclear regulatory framework involved the preparation of an extensive Deterministic Safety Analysis (DSA) to obtain a licence to operate a reactor. The DSA's process essentially is structured as follows: determine the design requirement, add a significant safety margin based on engineering experience, and then show that the energies available in the system cannot exceed that safety margin. For example, we know the design pressure of a given pipe, we make the pipe strong enough to withstand several times that pressure, and then we show that the system can never achieve a pressure that high. The objective of the DSA was to demonstrate that, with the safety analysis prepared employing the current design of the reactor, the overall response of the reactor to abnormal events ("transients") and accident conditions was not to exceed limits established in the Licence, and hence, the required protection of the workers, members of the public and environment was assured.

In the 1980s, probabilistic tools were developed and formalized into what is now known as PSAs (previously called Probabilistic Risk Assessment or PRA). Many Canadian researchers figured prominently during the development period of the PSAs, placing Canada at the leading edge in this area. Since then, the Nuclear Industry has prepared a number of PSAs for its reactors as it is a very useful tool for looking at safety in a different way than deterministic analysis. It provides insights on risks and assists in making decisions on what is acceptable in operating a plant. This is a fact also recognized by the federal regulatory body of nuclear power in Canada, the Canadian Nuclear Safety Commission (CNSC) by the issuance in 2005 of the Regulatory Standard S-294, *"Probabilistic Risk Assessment*", which later became part of the regulatory framework. More recently, the S-294 has been superseded by the Regulatory Document REGDOC-2.4.2, *"Probabilistic Safety Assessment for Nuclear Power Plants"*.

The results of PSA analysis are compared against Safety Goal Limits established first by the industry and later accepted by the CNSC, and against tighter internal safety goal targets which nuclear power plant operators may use to drive continual risk reduction efforts. In general, PSAs complement deterministic safety analyses.

What’s a PSA?

In short, a PSA is a tool that provides an overall review of the adequacy of the safety of the current station design and operation for each nuclear power station. The PSA is a comprehensive model of the plant that incorporates knowledge about plant design, operation, maintenance, testing and response to abnormal events. PSA is based on the idea that the product of the frequency of occurrence of an event and the consequence of the event, (i.e. the risk) represents a useful and meaningful quantity. For example, low frequency of event (lightning striking your car) times low consequence (a car is well insulated from ground by rubber tires) equals very low risk of you being hurt by lightning while sitting in your car. On the contrary, a high frequency example of a problem occurring while climbing Mt. Everest times high consequence (many bad possible results) make this a high risk activity. These risks can be compared, and decisions made about acceptability of risks.

Risk provides a means of quantifying the degree of safety inherent in a potentially hazardous activity as well as common basis for comparing the relative safety of dissimilar types of activities and industrial processes. One of the principles of the PSA process is that the larger the numerical value of the risk for a particular event or combination of events, the more important the event is to safety. Thus, a PSA represents a process by which risk is quantified, leading to the identification of the dominant contributors to risk. The knowledge gained is then used to create strategies to reduce risk and improve safety.

It is important to note that the focus of PSA analysis is generally to assess the risk of the most serious consequences for a nuclear power plant. These are typically grouped in two categories: severe reactor core damage (severe damage to most of the fuel, loosely called a “meltdown”), and a large release of radioactive material to the surrounding public and environment. PSA analysis of severe core damage is called “Level 1”, and analysis of large releases of radiation is called “Level 2”.

2015 Darlington NGS PSA Update

The 2015 Darlington NGS PSA update started with a Hazard Screening Assessment performed to confirm which hazards can be removed from further analysis, and identify which hazards need to be assessed in detail by a PSA. Events which are included in the assessment can be those internal to the plant, (such as steam line breaks, small and large loss of coolant accidents, total loss of power, fires inside the plant, etc.), and external events (earthquake, severe weather, solar flares, etc.). This approach is typical of PSAs and is consistent with methodology accepted by the CNSC. Fundamentally, certain extremely improbable events are removed (“screened out”) of further detailed assessment if the screening assessment determines that the probability of occurrence makes them an extremely small contributor to overall risk. An example for a nuclear power plant in Ontario might be a sandstorm – these just don’t happen in Ontario. However, a sandstorm would probably not be screened out for a nuclear station in some countries in the Middle East.

The preparation of a detailed PSA analysis starts with the identification of Initiating Events which could challenge reactor operation or fuel integrity, and ultimately result in severe core damage or a large release. Then, an Event Tree is developed in which, beginning from the selected initiating event and the systems credited in the mitigation of the event, the branches of the tree are built using logic. Every split of the tree branches represents a decision point where it is assumed that the mitigating system will either operate as per its design (success) or will not operate (failure) due to an equipment malfunction or human error. The end of a branch is reached when all the systems have been evaluated. Therefore, each branch in the Event Tree depicts a sequence of possible combinations of events between the Initiating Event and the end result; the possible combinations range from a successful outcome in every point to a failure in every decision point, and possible combinations in between those two extremes.

The probability of either success or failure in every decision point is estimated with additional Fault Trees, which are very detailed modeling of the system involved. These models include main components of the system (e.g., pumps, motors, heat exchangers, valves, etc.) and their support systems (electrical power, air supply, instrumentation and control, etc.), redundancies, operating procedures and human intervention. Another very important part of the model is the expected failure rates of the components, which is based on past experience. Fault tree analysis is a deductive, systematic way of performing failure analysis whereby an undesired state (a failure) of a system is specified, and the system is analyzed in context of its environment and operation to find all credible ways in which the undesired state can occur.

Once the estimate of failure of each decision point is completed, the total quantification of each branch in the Event Tree can be obtained. In a typical Level 1 PSA analysis, the branches of the Event Tree are binned into nine different so-called "Fuel Damage Categories" (FDC). The possible outcomes include the most severe involving failure to shutdown the reactor (FDC1) to the relatively benign where there are no fuel failures (FDC9). The results presented for the different Level 1 PSAs in Table 1 below represent the frequency of the most severe FDC: FDC1 and FDC2 – what we earlier called "severe core damage". The impact from the less severe events FDC3 through FDC7 only contributes much smaller values to the overall risk.

Thus, the goals of the Level 1 PSA is to identify occurrences at the plant that can cause a transient that would challenge fuel cooling, identify what systems can be credited to mitigate the event, assess what the impact of the transient may be on the mitigating systems, and to determine and quantify the degree of fuel damage that would occur if the mitigating systems were to fail.

If the fuel has been damaged, there is the potential for radioactive material to be released from the fuel into the "containment" structure of the nuclear plant. The design of Canadian nuclear power stations includes a so-called containment system to contain radiation released from the fuel, and thus prevent the release of any radioactive material from being discharged into the environment. A Level 2 PSA uses the information obtained from the Level 1 PSA to analyze potential system failures and accident phenomena that might result in a release to the environment, and the timing and magnitude of the release. The branches of the Containment Event Trees are binned into eight so-called "Release Categories" (RC), ranging from very large releases in RC1 to normal containment leakage in RC7. (In practice, a reactor containment structure is maintained at sub-atmospheric pressure to minimize releases to the environment from normal operations, however, a very small amount of air transfer out of containment does occur. This is called "containment leakage" and is monitored to ensure it is below strict limits.) Release Category RC8 is used to represent an event with significant internal building containment damage but where no releases to atmosphere occur. The Level 2 PSA results in Table 2 below represent the Large Release Frequency defined as the sum of RC1 through RC3. As with severe core damage, RC4 through RC8 contribute much smaller values to the overall risk.

At this point, a short note on scientific notation: Tables 1 and 2 below, present risk in units of "x10^{-5} occ/reactor-year", the number 10^{-5} means 1 in 100,000 or 0.00001, and "occ" means "occurrences". So for example, if the table shows "0.23" it is actually 0.23x10^{-5} occurrences per year of reactor operation, or a frequency of 2.3 events in one million years of reactor operation. At a station like Darlington with four reactors, one year of time represents four years of reactor operation. Also note that the result is not a prediction. It is not saying that an event WILL occur, say, 9.2 times in a million years, or that it won't occur in the next 10 years. It is an assessment that such an occurrence is very unlikely, and less likely than an event with a higher frequency of occurrence.

Thus, a nuclear PSA identifies the various sequences that lead to radioactive releases, assigns them to different categories of consequences, and calculates their frequencies of occurrence. The results of the Level 1 and Level 2 of each PSA hazard are compared against the Safety Goal Limits called Severe Core Damage Frequency (SCDF) and Large Release Frequency (LRF), whose numerical values are 10^{-4} occ/reactor-year and 10^{-5} occ/reactor-year, respectively. The intent of these Safety Goal Limits is to ensure that the potential radiological risks arising from nuclear accidents associated with the operation of nuclear power reactors are low in comparison with the risk to which the public is normally exposed. The results of the different PSA elements have never exceeded the numerical value of the Safety Goals Limits.

Over time, nuclear power plant operators identify opportunities to improve the safety of the plant. This may result from analysis of our own events, events at other plants like Fukushima, or from regulatory requirements to perform environmental assessments of projects such as plant modifications or refurbishments. Two such examples are referred to in the tables provided below. One, called "EME" or Emergency Mitigating Equipment, has been implemented as a result of the Fukushima event in Japan. EME is a set of portable diesel generators, pumps and hoses which could be used, in addition to existing designed plant equipment, to provide additional, flexible, redundant means of cooling to the fuel. Another, "SIOs" or Safety Improvement Opportunities, represents five major safety enhancement projects which OPG plans to undertake as part of the refurbishment of our Darlington station.

Results of the 2015 Darlington NGS PSA Update

OPG has recently completed the 2015 PSA update for Darlington Nuclear Generating Station. It is called DArlington Risk Assessment or "DARA" for short. Details of the update can be found in the OPG report NK38-REP-03611-10072, "*Darlington NGS Probabilistic Safety Assessment Summary Report"*, available on the OPG.com website.

The 2015 Darlington NGS PSA results for both Level 1 and Level 2 are reproduced in the Tables 1 and 2 below.

Table 1 provides the PSA Level 1 results for the different hazards considered in the 2015 PSA update. The first column identifies the six hazards for which a PSA needed to be prepared. The second column show the updated results for the case of "Baseline including the benefits of EME", which build up on the results obtained in the Darlington NGS 2011 PSA. The last column presents the results with the benefits of both EME and SIOs added to the Baseline.

Table 1. Level 1 - Severe Core Damage Frequency results.

Level 1 - Severe Core Damage Frequency (x10^{-5} occ/reactor-year)		
PSA Hazard	2015 DARA Baseline (with EME)	2015 DARA Baseline (with EME and SIOs)
Internal Events at Power	0.23	0.14
Internal Events during Outage	0.10	0.05
Fire at Power	0.09	<0.09
Flood at Power	0.02	<0.02
Seismic Event at Power	0.37	0.14
High Winds at Power	0.22	0.08
Unit SCDF Aggregated across all hazards	0.93*	0.47*
Safety Goal Limit	10	10

Note that numbers extracted from the table must be multiplied by 10^{-5}.
(*) The aggregate LRF excludes the LRF for Internal Event during Outage since the Internal Events at Power results are bounding and assume that the unit is at full power 100% of the time.

It should be noted that the result of each PSA is well below the Safety Goal Limit of SCDF, sometimes by at least a factor of 25, or much more, up to 500. That means that the design of the Darlington reactors is so robust that the possibility of failure of the systems credited to mitigate a transient created by the initiating event which may challenge core cooling is extremely low. Hence, the risk posed by any given hazard is much lower than other risks to which the public is exposed.

Note that the right column includes the results for Fire and Flood at Power with "less than" signs to indicate that a full assessment was not prepared since the design of the SIOs had not been completed by the time this PSA update was prepared, however, it is anticipated that future results for Fire and Flood will demonstrate a further reduction in risk. The SIOs that play a significant role in the Level 1 PSA are the Powerhouse Steam Venting System (PSVS), the third Emergency Power Generator (EPG), and the emergency make-up water supplied by new firewater pumps. Future PSA model updates will reflect the actual design and operation of these SIOs with better accuracy.

More recently, a suggestion to add up the results of all the hazards considered in the PSA has been proposed as a measure to estimate the "aggregate" risk. Much debate has ensued among PSA practitioners about the correctness of the proposal since each PSA is prepared with different methodology, different modeling, uncertainties and assumptions. In addition, since there are no “official aggregated Safety Goal Limits", the interpretation of the results of a direct aggregation becomes difficult. Nonetheless, Table 1 shows the results of Unit SCDF Aggregated across all hazards, which compare very well against the existing per-hazard Safety Goal Limit, given the lack of a better comparator.

Table 2 below shows the Level 2 results for the different hazards considered in the 2015 PSA update, and as before, the second column presents the results for the “Baseline including the benefits of EME”, and the last column, the results of “Baseline and benefits of both EME and SIOs”.

Table 2. Level 2 - Large Release Frequency results.

Level 2 –Large Release Frequency (x10^{-5} occ/reactor-year)		
PSA Hazard	2015 DARA Baseline (with EME)	2015 DARA Baseline (with EME and SIOs)
Internal Events at Power	0.10	0.04
Internal Events during Outage	<0.10	<0.05
Fire at Power	0.08	<0.08
Flood at Power	0.02	<0.02
Seismic Event at Power	0.28	<0.14
High Winds at Power	0.10	0.05
Unit LRF Aggregated across all hazards	0.58*	0.33*
Safety Goal Limit	1	1

Note that numbers extracted from the table must be multiplied by 10^{-5}.
(*) The aggregate SCDF excludes the SCDF for Internal Event during Outage since the Internal Events at Power results are bounding and assume that the unit is at full power 100% of the time.

As noted, the result of each PSA is well below the Safety Goal Limit of LRF, sometimes by a factor of 10 or more, up to 50. That means that the design of the Darlington containment system is so robust, that the possibility of releasing radioactive material onto a populated area as a result of containment failure or malfunction is extremely low.

The middle column includes the result for Internal Events during Outage with a "less than" sign to indicate that a full assessment was not prepared in detail since a large release can only occur if severe core damage has occurred. So, the large release frequency while the unit is in outage can be bounded by the already low frequency of the severe core damage while the unit is in outage, i.e. LRF must be less than SCDF.

The right column includes the results of Internal Events during Outage, Fire, Flood and Seismic Event at power with "less than" signs to indicate that a full assessment was not prepared since the design of the SIOs had not been completed by the time this PSA update was prepared, however, it is anticipated that future results will demonstrate a further reduction in risk. The SIOs that play a significant role in the Level 2 PSA and in the management of severe accidents are the Containment Filtered Venting System (CFVS) and Shield Tank Overpressure Protection (STOP) modifications. Future PSA model updates will reflect the actual design and operation of these SIOs with better accuracy.

Similarly, Table 2 shows the results of Unit LRF Aggregated across all hazards, which also compare very well against the Safety Goal Limit.

Each of these PSA results were derived by applying a scientific methodology which involves the necessary assumptions and models. Methodologies are routinely revised and improved every few years, and PSA results may change from one update to the next even if both the design of the plant and its operation have not changed. Thus, some care must be applied when interpreting the PSA results. A widely accepted interpretation of the PSA results is to consider them as indicators, which in general terms their numerical value must be lower than the Safety Goal Limits.

This approach to PSA results avoids a narrow focus of pursuing a very low result at all costs because of the misconception that nuclear power plants are unsafe unless the numbers are exceedingly small.

Risk-Based versus Risk-Informed

On numerous occasions it has been strongly requested in Licensing Hearings that a nuclear power station be shutdown because a PSA results were not perceived to be low enough; the main cited reason has been that the station was unsafe to operate. However, this point of view highlights a common misapplication of PSA results.

PSA tools were never intended to be the only mechanism for making a Risk-Based decision that is, making a complex decision based solely on the numerical result of an assessment. For example, if the result obtained is lower (or higher) than a prescribed criterion, then the decision is to proceed (or not to proceed) or something similar. That is not a process followed while operating a power station, and actually, not even followed in our personal lives since we need to know much more than the result of a simple tossing of a coin to make a decision.

The PSA results are used by the Nuclear Industry as part of a Risk-Informed Decision Making process, where the PSA results are only one of many other input parameters needed and evaluated prior to making a decision. Thus, the PSAs are not magic tools producing “the answer”. They are not providing the "decisive factor" or the "final answer" on safety; they don’t determine whether something is safe or unsafe. Rather, they are useful tools providing valuable information which will be part of a larger set needed to make a good decision.