# Insights and Improvements Based on Updates to Low Power and Shutdown PRAs

**J. F. Grobbelaar, J. A. Julius, K. D. Kohlhepp, & M. D. Quilici,**
Scientech, a Curtiss-Wright Flow Control Company, Tukwila, WA, U.S.A.

**Abstract:**

In several countries, the requirements for probabilistic risk assessments have increased beyond a Level 1 internal events PRA to add or address spatial and external hazards. In a growing number of countries the requirements have further increased to address all Level 1 hazards in all plant operating modes. Scientech developed its first shutdown probabilistic risk assessment (PRA) in the early 1990s for a European nuclear power plant. Since then several additional low power and shutdown PRA models were developed in the United States following the same approach. The original shutdown PRA model was expanded to evaluate hazards challenging fuel in the reactor vessel and fuel in the spent fuel pool; modeling Level 1 core damage for all hazards in all plant operating modes, with corresponding Level 2 (release) and Level 3 (consequence) models. This complete PRA of all hazards and all modes was incorporated into the European plant's licensing basis, and in 2010 a peer review was conducted.

In the last three years, the shutdown PRA model was updated and a follow-on peer review conducted. Plant operational state definitions were revised to better agree with technical specifications governing the plant operating modes. Additional initiating events were modeled for the fuel pool plant operational states as well as the refueling plant operational states. Initiating event frequencies have been updated to reflect recent operating experience. Success criteria and accident sequence development were revised based on insights from new thermal-hydraulic analyses. New shutdown procedures and "FLEX" strategies were considered in the accident sequence development. New operator actions were credited and human reliability analyses were performed. During the same period, additional model changes and refinements were developed on the USA shutdown PRA models.

This paper presents the insights and improvements made in the PRA modeling of low power and shutdown states, and also presents a summary of insights and benefits that the plant obtained during the development and updates of the underlying shutdown PRA models.

Key Words: Shutdown PRA, Shutdown PSA, Low Power and Shutdown

## 1. INTRODUCTION

In several countries, the requirements for probabilistic risk assessments (PRA) have increased beyond a Level 1 internal events PRA to add or address spatial and external hazards. In a growing number of countries the requirements have further increased to address all Level 1 hazards in all plant operating modes. Scientech developed its first shutdown probabilistic risk assessment in the early 1990s for a European nuclear power plant. Since then, several additional low power and shutdown PRA models were developed in the United States following the same approach. The original shutdown PRA model was expanded to evaluate hazards challenging fuel in the reactor vessel and fuel in the spent fuel pool; modeling Level 1 core damage for all hazards in all plant operating modes, with corresponding Level 2 (release) and Level 3 (consequence) models. This complete PRA of all hazards and all modes was incorporated into the European plant's licensing basis, and in 2010 a peer review was conducted.

In the last three years, the shutdown PRA model was updated and a follow-on peer review conducted. Plant operational state definitions were revised to better agree with technical specifications governing

the plant operating modes. Additional initiating events were modeled for the fuel pool plant operational states as well as the refueling plant operational states. Success criteria and accident sequence development were revised based on insights from new thermal-hydraulic analyses. New shutdown procedures and "FLEX" strategies were considered in the accident sequence development. New operator actions were credited and human reliability analyses were performed. During the same period, additional model changes and refinements were developed on the USA shutdown PRA models.

This paper presents the insights and improvements made in the PRA modeling of low power and shutdown states, and also presents a summary of insights and benefits that the plant obtained during the development and updates of the underlying shutdown PRA models. Section 2 of this paper provides background information about the scope and development of the shutdown PRAs. Section 3 of this paper presents insights into the plant operational state modeling, and Section 4 presents insights into the PRA elements.

## 2. BACKGROUND

In 2012 a complete shutdown probabilistic risk assessment (PRA) update was developed for the Borssele nuclear power plant (NPP) to update the original 1990's shutdown PRA. The update was conducted to address findings and observations from an International Atomic Energy Agency (IAEA) International Probabilistic Safety Review Team (IPSART) mission, and to improve the as-operated modeling of the plant in accordance with recent modifications and development of shutdown emergency operating procedures (EOPs) [1]. These plant improvements were conducted as part of the plant's continuing process to review and improve plant safety, and also to consider insights from the Fukushima stress test [2] and guidance provided in NEI 12-06 [3]. A summary of the scope of the PSA-2013 paper describing the extent of the Borssele Shutdown PRA changes is provided below.

> "The scope of the shutdown PSA update is a Level 1, 2 and 3 PSA including internal events and all hazards. The scope of this paper is limited to the Level 1 PSA. This paper provides some background in section 2, discusses the plant operational state (POS) definitions in section 3, initiating events in section 4, system modeling in Section 5, success criteria in section 6, accident sequence development in section 7, human reliability analysis in section 8, results and conclusions in section 9, and further work in section 10……
>
> The Borssele NPP is a single unit, 485 $MW_e$, 2 loop pressurized water reactor of Siemens KWU design. It is located in The Netherlands and has been operational since 1973. Notable features of this plant are a digital control room and "bunkered systems", which are additional systems - beyond the conventional standby engineered safeguard systems - designed to mitigate external events like large scale flooding. These systems include 380 VAC emergency power, 24 VDC power, reserve auxiliary feedwater, reserve decay heat removal, reserve cooling water, reserve high pressure injection, and a reserve spent fuel pool (SFP) cooling train. Unique to the Borssele NPP is shutdown EOPs. Pertinent to the shutdown analyses is that the SFP is located inside containment while the SFP cooling system is outside containment."

Also during the 1990's, shutdown PRA models were developed in the United States in order to address outage risk management considerations. Shutdown PRA models were developed for configuration risk management. These models were developed as an extension of the full power PRA model. Typically, full power probabilistic risk or safety assessments (PRAs/PSAs/IPEs) were already in existence for the nuclear power plant to be modeled. Additionally, the longer range goal was to be able to evaluate the risk in conducting plant maintenance in different plant states, such as to evaluate if the risk was less to remain at power rather than shutdown to cold shutdown to conduct maintenance. The general methodology used was consistent with the International Atomic Energy Agency guidance for the modeling of accident sequences during shutdown and low power conditions [4]. Further, other than the definition of outage types and plant operational states, the underlying methodology (small event tree, large linked fault trees), system models (fault trees) and data were the same as that typically used in the

full power PRAs/IPEs with the necessary considerations made for differences in plant response due to shutdown conditions.

## 3. PLANT OPERATIONAL STATE INSIGHTS

One of the major issues for a shutdown PRA address is the selection and modeling of plant operating states since this task sets the scope of the shutdown PRA. A full power PRA consists of one plant operating state (POS). Because plant system alignments (both operating equipment alignment and also the equipment out of service) change frequently throughout the outage, there are potentially thousands of plant operational states to model. Additionally, the POS requirements vary depending on the type of outage. For example, a quick shutdown to hot standby consists of different POS's than a refueling outage. Similar to the initiating event task in a PRA, the goal of this task is to identify, group and quantify the characteristics, frequency and duration of the modeled POS's.

The recommended modeling practice is to select POSs for fuel in the reactor pressure vessel (RPV) based on plant Technical Specification (TS) operating modes. The primary benefit is to be able to easily link the PRA to the outage schedule, and to improve the understanding when talking to plant operations and maintenance staff. Whereas the POS concept is typically limited to PRA practitioners, the concept of Technical Specification operating mode is widely known to plant staff. This advantage is summarized in the draft USA LPSD PRA Standard [5]:

> *"Several plant conditions could be used to define a POS, but model understanding and configuration control are facilitated when the set of plant conditions chosen is consistent with those used by plant personnel to govern LPSD operations (i.e., plant operating modes or operating conditions as defined in plant technical specifications)".*

The 2012 update of the European model eliminated "low power" from the shutdown analysis, as the power POS was extended to apply and provide a bounding analysis whenever the core is critical. In the previous version of the PRA, "low power" was included in hot steaming POS, which was the part of the shutdown/startup evolution between criticality and approximately 15% reactor power while the turbine generator is not synchronized to the grid and house loads are powered from the startup transformers and not the generator transformer. The new definitions of the power and hot steaming POSs resulted in simplified event trees for the hot steaming POSs, since reactor trip and RCS pressure control were not needed. In both the European and USA shutdown models, the "low power" portion of the model was typically not used, as the success criteria for safe shutdown components during this state were bounded by those for full power.

Also during the 2012 update of the European model, the POS boundaries of the shutdown states using residual heat removal shutdown cooling (RHR-SDC) were revisited and refined to better match refueling outage practices and recent changes to the plant's shutdown emergency procedures. Thermal hydraulic calculations that were conducted with the RPV head on, RPV head off, and RPV vents open and closed were reviewed to understand the impact on Level 1 plant response success criteria. The original 1990's model considered RPV with vents open to be equivalent to RPV with head off (based on thermal hydraulic analysis done in the 1990s), which is good for Level 1, but may have different Level 2 consequences. At that time, vents were assumed to stay open once opened, but since then new procedures have been developed that instruct closing of the vents on loss of RHR-SDC, so RPV vent status is now questioned in midloop sequences with RPV head on. Additional POSs model the state with RPV head off.

In the USA, similar POS refinements have been conducted based on insights from thermal-hydraulic analyses. For example, for some Westinghouse PWRs when the refueling basin is flooded and the RPV upper internals are installed, there are limited connections between the refueling basin and the RPV such that the RCS behaves as if the extra volume of water in the refueling basin is not available for cooling using natural circulation flow. During this portion of the refueling basin flooded POS, the

PRA success criteria have been reviewed to ensure natural circulation is not available as a long term success state for decay heat removal.

In both Europe and the USA, following the Fukushima Daiichi event, the Spent Fuel Pool (SFP) has received increased attention. A SFP POS has been part of the European and USA models since the early 1990s. In the 2012 European update, the SFP POS was explicitly modeled as two states, one defined as fuel pool early (FE) and for fuel pool late (FL). While POS FE corresponds directly with a specific Technical Specification mode, the Technical Specification does not define a mode for SFP following completion of core reload (POS FL). POS FL was defined to address the spent fuel in the SFP while the "active" core is in the RCS until the next core offload. A new POS to model reshuffling outages (outage without a complete core unload where approximately one third of the core is replaced and the core reconfigured while the SFP and reactor cavity remain connected) was investigated, but it was concluded that the reshuffling outage is adequately represented by POS's for Core Offload and Core Load.

In both Europe and the USA, the strategy and management of plant outages has changed, requiring review in order for the PRA to properly reflect current plant practices. The trend has been for longer intervals between refueling outages and shorter refueling outages. In a PRA that captures an "average" or typical year, the historical data for the preceding 5-10 years should be reviewed in order to check and update (if appropriate) the calculated POS durations and annual fractions. In the application of the shutdown PRA to configuration risk management, such as the usage of the USA models as well as the European model, then the duration and configuration of the plant states is provided by the outage schedule.

## 4. PRA TASK INSIGHTS

### 4.1 Internal Initiating Events

The internal initiating events typically identified and considered in the PRA modeling of shutdown POSs are summarized in Table 1 below.

**Table 1 - Shutdown Initiating Events in Each POS**

| Category | Initiating Event POS: | Hot Steaming | Cold Shutdown (RHR) | Mid loop (RHR) | Core Offload Load | Spent Fuel Pool |
|---|---|---|---|---|---|---|
| Transients | Loss of Offsite Power | X | X | X | X | X |
| | Single SGTR (PWR) | X | | | | |
| | Steam/Feedwater Line Break | X | | | | |
| | Loss of Main Feedwater | X | | | | |
| | Loss of SFP Cooling | | | | X | X |
| | Loss of RHR-SDC | | X | X | X | |
| Loss of Support Systems | Loss of DC Buses | X | | | | |
| | Loss of High Voltage AC Bus | X | X | X | X | X |
| | Loss of Instrument Buses | X | X | X | | |
| | Feedwater Tank Rupture | X | | | | |
| | Loss of component cooling water system/s | X | X | X | X | X |
| | Loss Low Voltage AC buses | | | | X | X |
| LOCAs | ISLOCA via RHR Suction | X | | | | |
| | ISLOCA via LPSI Inj. Line | X | | | | |
| | Flow diversion from RHR | | X | X | | |
| | RHR pipe LOCAs | | X | X | X | |
| | SFP LOCA | | | | X | X |

**Table 1 - Shutdown Initiating Events in Each POS**

| Category | Initiating Event POS: | Hot Steaming | Cold Shutdown (RHR) | Mid loop (RHR) | Core Offload Load | Spent Fuel Pool |
|---|---|---|---|---|---|---|
| | Large LOCA/RPV rupture | X | | | | |
| | Intermediate LOCA | X | X | | | |
| | Small LOCA | X | X | X | X | X |
| | Very Small LOCA | X | X | X | X | X |
| Special | Extreme grid disturbance | | | | X | X |

In developing the list of internal initiating events, the following insights should be noted.

- Transient losses of decay heat removal apply to all POSs, but are typically not significant during shutdown with the refueling basin flooded (core offload/load).
- Support systems affect decay heat removal, and should be considered, especially where the support system potentially affects fuel in the RPV as well as fuel in the Spent Fuel Pool.
- Losses of inventory (shutdown LOCAs) apply to all POSs, and reduce the advantage of the additional inventory that is initially available at the start of the refueling basin flooded (core offload/load) and Spent Fuel Pool POS's.
- Losses of inventory outside of containment can occur such as with certain RHR-SDC breaks, and thus contribute to interfacing systems LOCA (where the RCS sump is not filled and a pathway exists that breaches containment).
- Initiating event frequencies have been updated to reflect recent operating experience. Since the early 1990's there has been a significant reduction in the frequencies associated with a loss of decay heat removal.

### 4.2 External Hazard Events

A significant comment from the Peer Review of the European shutdown PRA was that the hazard screening had not been reviewed and updated for many years. After a screening process, the internal and external hazards in Table 2 were included in the modeling of the European shutdown PRA.

**Table 2 - Hazards Included in the European Shutdown PRA**

| | |
|---|---|
| **Internal Hazards** | Internal flooding |
| | Internal fire |
| | Failure of pressure parts, supports or other structural components, including HELB |
| | Disruptive failure of rotating machinery or other equipment |
| | Dropped or impacting loads |
| **External Hazards** | Tornado/high winds |
| | Meteorite |
| | High water level |
| | Explosion after transportation accident (ships transporting LNG and ammonia) |
| | Chemical release after transportation accident: toxic clouds |
| | Missiles from off-site activity (e.g. military, (wind / steam turbines) |
| | Aircraft crash |
| | Earth quake (analysis on going) |

The following insights were developed in Reference 1.

> "Given the Fukushima accident, special attention was given to combinations of hazards. Looking at the (screened in) hazards the following can be concluded on credible combinations. High wind and flooding are always combined, as high wind (storm) is a precondition to cause the high water levels that could threaten the plant. The consequences of storms during a flood are bounded by those for the flooding itself.
>
> High winds could cause shipping incidents. However, shipping incident statistics include those caused by storm. The possible consequences (flash fire, toxic clouds, explosion) envelope the possible damage by high winds. Furthermore, the high wind will dilute the chemicals that can be released from the ships; stable weather is needed for a shipping incident to develop into a threat to the plant.
>
> External flooding caused by an earth quake has been screened while tsunamis can be excluded. So there is no need to consider the impact of a flood wave on a plant that is already possibly damaged by an earthquake.
>
> Also the combination of the plant damaged by an earthquake and a flooding that is made possible by a dike that is damaged by the same earthquake is beyond consideration as there is still a storm surge needed to create a flooding. A damaged or failed dike in itself will not lead to site flooding as the site is 3 m above mean sea level (NAP), a normal tide is between – 2 m NAP and +2 NAP, and the all equipment that is susceptible for flooding is placed at a minimum elevation of +5m NAP.
>
> The combination of seismic damage to the plant and gas clouds originating from seismically damaged industry might need investigating, depending on the outcome of the seismic analysis that is being performed.
>
> The consequences of possible (internal) fires caused by explosions or aircraft impact safety are bounded by the consequences of the explosion or impact on the buildings: the complete loss of the building and the equipment inside."

### 4.3 Success Criteria

This is an element where all shutdown PRA models benefit in model review and refinement. Understanding the plant behavior following an initiating event is important to the development of the accident sequence (plant response) models as well as for the timing of operator recovery actions.

### 4.4 Accident Sequence Development

The insights from this PRA task are summarized below.

- New Shutdown Procedures. With increasing emphasis on the losses of RHR shutdown cooling in the USA and internationally, plant response procedures are being reviewed and updated. The shutdown PRA model should check current plant procedures to ensure the modeled plant response reflects the "as-operated" plant. In the European PRA, shutdown procedures included a shutdown diagnosis procedure, or in the Westinghouse terminology a shutdown E-0 (S-E-0) applicable during POS's with RHR-SDC. The S-E-0 procedure is unique to the Borssele NPP (to the best of our knowledge). Additionally, some modifications were also made to the SAMGs.

- Event Tree Updates for Internal Events. In many of the USA plants, the shutdown models were initially created by copying and adapting the full power PRA event trees. Thus, the

shutdown event tree models require review and update to re-synchronize with the full power models. This insight applies to both internal events, spatial events and external hazards.

- Defense in Depth Modeling. Many USA shutdown PRA models developed and focused on defense-in-depth models, especially for functions such as Reactivity Control that are not well suited to PRA quantification. These models work well for outage risk management as they match well with shutdown Technical Specifications.

- Post-Fukushima Insights. One of the insights of the Fukushima stress test of the European plant was that the available time to restore core cooling is very limited during mid-loop operation following a SBO. This was not really a new insight of course, but what is new is the requirement for a measure to reduce these consequences, irrespective of their likelihood. The measure had to be twofold: provision of the necessary procedure/s and training of the operators to perform these procedures.

### 4.5 Systems Modeling

The insights from this PRA task are summarized below.

- Additional systems such as Fire Protection Back-Up to Spent Fuel Pool are often added to the shutdown PRA models.

- Component test and maintenance modeling, including "disallowed maintenance" combinations should be reviewed to ensure they are consistent with the current outage practices.

- Unavailability of automatic actuation. The reactor protection system (RPS) modeling should be reviewed to ensure correct availability/unavailability of RPS signals according to the Technical Specifications applicable to each POS. RPS signal availability can vary, for example into one of three groups: 1) available at power and hot shutdown only, 2) available at power, hot shutdown, cold shutdown, and midloop, 3) available in all POSs. The enabling/disabling of RPS signals for different POSs is typically accomplished using house events.

- Consistency with full power system fault trees. In many of the USA plants, the shutdown models were initially created by copying and adapting the full power PRA fault trees. Thus, the shutdown fault tree models require review and update to re-synchronize with the full power models (or merge the two models). In the European PRA update, for example, the common cause event identification update for full power was propagated into the shutdown PRA model.

### 4.6 Human Reliability

The shutdown HRA models developed for the USA PRAs as well as the European shutdown PRA included detailed analysis for many HFEs including fire HFEs. These studies showed that that in most cases that current HRA methods are appropriate, but it also confirmed that a weakness of available HRA methods is their ability to model recovery actions with very long time windows (available time). The insights from the shutdown HRA task are summarized below.

- Identification. A shutdown HRA update starts with identification of operator actions modeled as human failure events (HFEs) in the shutdown PRA. The identification task starts with a review of the current identification and grouping of all human failure events already modeled by POS. The HRA task then reviews any new procedures and incorporates new actions into the PRA model on an as needed basis. If applicable, the review should also include

identification of all instrumentation required for each shutdown action credited in the fire PRA.

- Quantification. The quantification of each HFE followed the "EPRI HRA Approach" as implemented in the EPRI HRA Calculator [6]. The CBDTM and HCR/ORE [7] quantification methods were used. However, these methods were developed for at-power, EOP driven actions which are typically required within the first couple of hours of an initiating event. In the shutdown model there are many actions in which the time available can be on the order of days and the lower bound quantification limits of the methods are reached. The shutdown HRA applied a lower bound of 1E-6 for individual actions. In some cases these lower bound HEPs are risk significant and there is currently no available HRA method which can be used to systemically justify lower HEP values. Additionally, the currently available HRA methods do not provide guidance on how to apply recoveries from off-site given the long time available. It would seem reasonable to take credit for these additional long term recovery factors, but there is no available guidance on the consistent treatment for such long term recovery factors.

- Spatial Events. For the shutdown fire HRA of the European PRA, the guidance in NUREG-1921 [8] was followed. Although this guidance was intended for at-power applications, in general it remained applicable for shutdown fire HRA. The insight from the fire HRA was that in many cases the fire was extinguished hours before the actions were required, and the fire would have little to no impact on the operators' performance. For each fire HFE, the instrumentation cabling was verified or traced to ensure that the fire impact on cues and indications was understood. Due to the redundancy and diversity in cues and indications, very few shutdown actions were significantly impacted by fire.

- Dependency After the individual HEPs were quantified and implemented into the PRA model, a dependency analysis was performed by review all combinations of HFEs, for each POS. Common cognitive HFEs were developed for actions which are based off the same procedure transfer or same cue. In the Spent Fuel Pool POS, almost all operator actions share a common cognitive for diagnosis of loss of SFP cooling. In this plant state, there is at least 6 hours available for diagnosis and multiple redundant cues and indications including SFP cameras. This risk significant common cognitive applies the lower bound HEP and due to the exceptionally long time window this action was considered to be independent from all other actions in the combinations.

## 5. SHUTDOWN PRA RESULTS AND CONCLUSIONS

In several countries, the requirements for probabilistic risk assessments have increased beyond a Level 1 internal events PRA to address all Level 1 hazards in all plant operating modes. Scientech developed its first shutdown probabilistic risk assessment in the early 1990s, starting with a European nuclear power plant. This European PRA was used to communicate average, annual risk as well as to provide the plant a tool for outage risk management. Several shutdown PRA models were then developed in the USA, primarily for use in outage risk management.

In the last several years, many of these shutdown PRA models have undergone review and update. Plant operational state definitions were revised to better agree with technical specifications governing the plant operating modes. Additional initiating events were modeled for the fuel pool plant operational states as well as the refueling plant operational states. Initiating event frequencies have been updated to reflect recent operating experience. Success criteria and accident sequence development were revised based on insights from new thermal-hydraulic analyses. New shutdown procedures and "FLEX" strategies were considered in the accident sequence development. New operator actions were credited and human reliability analyses were performed.

The updated shutdown PRAs have been used to evaluate risk-significance and for outage risk assessment. The improvements in the shutdown PRA models have been used to provide the following benefits to the plant.

- Defense-in-depth (qualitative) modeling facilitates outage risk management, especially for functions such as Reactivity Control that are not well suited to PRA quantification. These models work well for outage risk management as they match well with shutdown Technical Specifications.

- Ability to evaluate risk-significance of shutdown events and issues (e.g. significance determination process in the USA).

- Ability to quantify and evaluate risk trade-offs of conducting maintenance in different POSs (e.g. the risk of staying online for maintenance as opposed to shutting down).

- Ability to conduct outage risk assessment and outage risk management.

- Ability to evaluate proposed plant improvements (hardware and procedure changes).

Current PRA methods, especially HRA, do not lend themselves to modeling very long term scenarios. In the case of loss of SFP cooling, the time to core uncover can be several days following a transient loss of decay heat removal. During this time, there will be many opportunities for repair and/or recovery from both onsite and offsite sources in accordance with the FLEX concept, but the offsite sources are not currently credited due to the shortcomings of the PRA methodology. It would be useful in future if the PRA methodologies can be developed or strengthened so that long term scenarios can be modeled with less uncertainty, or eliminated from the model.

## 6. REFERENCES


[1] *Shutdown Probabilistic Safety Assessment Update*, Erik Roose et al, presented at PSA 2013, American Nuclear Society sponsored Probabilistic Safety Assessment Conference, Columbia, SC, September, 2013.

[2] *Final Report Complementary Safety Margin Assessment NPP Borssele*, EPZ, October 31, 2011.

[3] *Diverse and Flexible Coping Strategies (FLEX) Implementation Guide*, NEI, Suite 400, 1776 Street NW, Washington, D.C., May 2012

[4] *Working Material, Guidelines for Shutdown Risk Assessment*, Report of a Consultants Meeting Organized by the International Atomic Energy Agency, Vienna Austria, 1994.

[5] ANSI/ANS-58.22-2012, American National Standard Low Power and Shutdown PSA Methodology

[6] *The EPRI HRA Calculator® Software Users Manual*, Version 4.2, EPRI, Palo Alto, CA, and Scientech, a Curtiss-Wright Flow Control company, Tukwila, WA, EPRI Software Product ID #: 1021230: 2007.

[7] *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment*, EPRI TR-100259, EPRI, Palo Alto, CA: 1992.

[8] EPRI/NRC-RES Fire Human Reliability Guidelines, NUREG-1921 Final Report, US NRC and EPRI, July 2012.