Risk-Informed PSA Applications within the Belgian Nuclear Context – Findings and Insights

Van Opstal Filip[1]*, Agosti Federico[2]

[1]Tractebel ENGIE, Brussels, Belgium
[2]Tractebel ENGIE, Brussels, Belgium

ABSTRACT

A nuclear phase-out law has been in effect since 2003 in Belgium, limiting the lifetime of nuclear power plants to forty years. Two units – Doel Unit 3 and Tihange Unit 2 - had their final shutdown in 2023. An exception has recently been granted for the two youngest Belgian nuclear reactors (Tihange Unit 3 and Doel Unit 4) allowing 10 additional years of operation in addition to prior exceptions granted for Tihange Unit 1 and Doel Units 1 & 2. In preparation of the definitive shutdowns of Doel 3 and Tihange 2 and long-term operation of Doel 4 and Tihange 3, Tractebel ENGIE (responsible designer) and ENGIE Electrabel (plant operator) have pursued an Integrated Safety Approach (ISA). The engineering consultancy firm Tractebel was involved in the design and construction of the nuclear power plants in Doel and Tihange. ENGIE Electrabel is an electricity and natural gas provider in Belgium and owner/operator of the Nuclear Plants of Tihange and Doel. Tractebel ENGIE and ENGIE Electrabel are both owned by the French multinational ENGIE.

With respect to units undergoing shutdown, all safety impacts of the proposed post-operational phase (POP) configuration changes were evaluated in an integrated way, in a manner that complements both the deterministic approach and engineering judgment with adequate risk information. PSA practices were developed to allow reflection of changes to system/component classification and (partial) abandonment of systems. Additionally, a PSA aided Defense-in-Depth evaluation was performed.

For the units retained for lifetime extension (LTE) an evaluation of the impact of potential Design Upgrades was performed, providing risk-reduction ranking and insights on dependencies between improvements.

Risk-informed frameworks have gained international traction in particular with respect to new builds. Evidence of this can be seen in the US license modernization project allowing a probabilistic first approach for licensing new non-light water reactors. The document highlights our experience gained with respect to using risk-insights to compare design alternatives whether being in the framework of a lifetime extension (addition of new safety features) or final shutdown of a unit (gradual reduction in safety systems). The paper focusses on the encountered hurdles and lessons learned, in particular the flexibility required in modelling when perusing models that can reflect different potential configurations to allow risk-ranking.

Keywords: *PSA, Internal Events, Post-Operational Phase, Spent Fuel Pool, Long-Term Operation, Defense-in-Depth, Risk-Informed Activities*

1. INTRODUCTION

* filip.vanopstal@tractebel.engie.com

Belgium has had a nuclear phase-out law in effect since 2003, which limits the operational lifetime of nuclear power plants to forty years. However, there have been historic exceptions granted for the two oldest Belgian nuclear plants: Tihange Unit 1 and Doel Units 1 & 2 and recently for the youngest units Tihange Unit 3 and Doel Unit 4. Doel Unit 3 and Tihange Unit 2 have reached the end of their qualified life without a planned LTE and were definitively shut down end 2022-early 2023.

Prior to the definitive shutdown of Doel Unit 3 and Tihange Unit 2, ENGIE Electrabel (operator) and engineering consultancy firm Tractebel ENGIE initiated activities to define and justify the necessary configuration changes of the remaining nuclear island during the post-operational phase (POP). After the shutdown, the spent fuel within the spent fuel pools (SFP) will need to be actively cooled for years, and the remaining nuclear island must support this operation. Further details about the Post-Operational Phase are provided in Chapter 2.

In pursuit of an Integrated Safety Approach (ISA), all safety impacts resulting from proposed changes to the Post-Operational Phase (POP) configuration were evaluated in an integrated manner. This approach complements both deterministic methods and engineering judgment, incorporating adequate risk information. The investigation explored alternative potential configurations from both deterministic and probabilistic perspectives, including sensitivity analyses to address sources of uncertainty. Notably, the analysis considered changes to system/component classification and focused on risks arising from internal events and seismic hazards. These assessments were built upon existing integrated Reactor-SFP (Spent Fuel Pool) Probabilistic Safety Assessment (PSA) models, with detailed considerations outlined in Chapter 3.

In addition to the more traditional applications of Probabilistic Safety Assessment (PSA) modeling, a PSA aided Defense-in-Depth evaluation was performed to re-evaluate the Design Basis Accident (DBA) levels by quantifying the frequency of postulated initiating events (PIEs) related to spent fuel pools. This analysis is elaborated upon in Chapter 4. The process of binning PIEs into different plant conditions has been revisited, along with the facility performance requirements resulting from this categorization. Furthermore, this paper discusses the role of PSA as a facilitator in such exercises.

As stated, recently long-term operation has been approved for the two youngest in order to meet the energy challenges of the future. These plants will be jointly owned by ENGIE and the Belgian state. In light of positive feedback from the stakeholders with respect to the aforementioned ISA to support POP, a risk-informed approach has also been applied with respect to the initial selection of potential design upgrades for the LTE of the newest units. These activities are described in Chapter 5. The paper ends with conclusions and main lessons learned in Chapter 6.

This paper provides an update to the work published earlier in the proceedings of 18th International Probabilistic Safety Assessment and Analysis (PSA 2023) hosted by ANS [6].

2. THE POST-OPERATIONAL PHASE AND NUCLEAR ISLAND CONFIGURATION

During the decommissioning phase, used nuclear fuel assemblies undergo a cooling period of approximately 4 years. This cooling process ensures that the assemblies are safe for subsequent

handling and loading into fuel containers. Once sufficiently cooled, the assemblies are gradually transported to the Spent Fuel Storage Facility (SFP) at the site.

As part of the decommissioning process, systems are planned for removal from operation. For the Doel 3 and Tihange 2 units, a global approach known as the "cold and dark" method is employed. Instead of dismantling systems individually, this approach involves shutting down all systems simultaneously. The primary objective of this study is to assess the risks associated with different options during this phase.

The blueprint for this activity includes identifying essential systems, structures, and components (SSCs) necessary to maintain safety and continue SFP operation. Abandoned systems are fully drained, de-energized, and, if needed, rinsed. For engines, fuel is removed from associated tanks and piping to reduce fire risk. Once fire loads related to halted systems are eliminated, the local fire extinguishing installation can be taken out of service. The 'cold and dark' approach further allows for justified removal of fire loads, such as active charcoal filters, considering Iodine-131's short half-life.

An optimization process aims to reduce operational costs by retaining a minimal number of equipment/trains. However, a clear risk objective is set: any reduction in trains or systems must not increase the risk to the SFPs compared to reactor operation, as quantified by the fuel damage frequency (FDF).

The following classification was defined for the nuclear island systems, structures, and components (SSCs) during the post-operational phase:

- **IPS-SAFE** (= SAFE A + B): These are SSCs that are "Important to safety" and are considered in the safety demonstration for design basis accidents.
- **IPS-FUNC A**: These SSCs are also 'Important to safety' but are not included in the SAFE category.
- **FUNC B**: These SSCs are not 'Important to safety' but are still requested to function.
- **ABAN**: These SSCs are no longer required to function.

Various scenarios were considered for the nuclear island configurations during the post-operational phase. These configurations originated from classifying SSCs based on their importance and defense-in-depth analysis all while applying graded approach. Up to four potential configurations each were retained for Doel 3 and Tihange 2, which were further validated using internal events SFP Probabilistic Safety Assessment (PSA) models. Seismic PSA analysis was performed for the final retained minimal configuration, while internal flooding and fire analyses were omitted due to their low initial risk contributions and the consideration of a 'cold and dark' approach.

3. PSA MODELLING ASPECTS FOR POP

This section focuses on the modeling considerations used to adapt the integrated reactor-SFP (Spent Fuel Pool) Probabilistic Safety Assessment (PSA) models for Doel 3 and Tihange 2. These

models were employed to evaluate the risks associated with the proposed post-operational phase configurations after the shutdown of these nuclear power plants.

2.1. Initiating Events

During the post-operational phase, specific initiating events (IEs) were carefully selected from the list of IEs considered in the Spent Fuel Pool (SFP) Probabilistic Safety Assessment (PSA) model. The following IEs were excluded due to the long-term post-operational regime:

- Pool Cooling Transients induced by Reactor Protection Signals.
- Pool Cooling System Ruptures with SFP connected to Reactor Building (RB) pools.
- Transfer Tube Rupture.
- Loss of cooling to RB pools.
- Rupture of the RB Pool liner.
- Primary Loss of Coolant Accident (LOCA) during Fuel Manipulations.
- Reactor Core Damage Sequences with Containment Failure.

Additionally, modifications were made to the Loss of Offsite Power (LOOP) frequency contributions. These adjustments account for the planned disconnection of the 380kV switchyard in all considered configurations and the extended scenario time windows due to residual heat levels in the spent fuel pools. Notably, the original spent fuel pool models, which included up to 8 operational phases, were simplified to a single operational phase for the post-operational regime.

2.2. Classification Changes

When it comes to functional equipment (FUNC) in nuclear facilities during the post-operational phase, it has been carefully evaluated the changed maintenance and testing regimes. This is particularly true for equipment transitioning to a functional status from a safe status. For all components transitioning to FUNC, the modelling of failure upon demand was changed from a periodically tested model to a repairable model. The latter means that the components are considered to operate until failure and they are consequently considered to be repairable with a fixed repair rate, selected based on plant and industry experience. However, the parameters used in the model have been penalized for more relaxed maintenance requirement and availability of spare parts for these components. That said, the failure rate of FUNC equipment was not penalized. Here are the key arguments supporting this approach:

- Continuity of Equipment:
  At the start of the post-operational phase, the equipment associated with declassified systems, structures, and components (SSCs) remains unchanged. Only over time could originally classified components be replaced by industrial-grade counterparts. It’s important to note that standard quality assurance practices (QA) are consistently applied.

- Failure Rates and Spare Parts:
  Most safety-grade components retained in the Probabilistic Safety Assessment (PSA) model exhibit failure rates in the range of 1E-5 to 1E-6 per hour. This translates to mean times to failure spanning from a few years to multiple years.

Abandoned trains serve as spare parts for the remaining operational train. Consequently, it is unlikely that original safety-grade components will contain non-QA parts by the end of the expected 4-year post-operational phase.

- Functional Operation and Sensitivity Study:
  FUNC components must remain operational during normal conditions. While there may be reductions in design specifications for replacement parts (considering post-accidental and lifespan aspects), pre-accidental operation remains largely unaffected.

  A sensitivity study assessing failure rates for post-accidental operation demonstrated limited sensitivity within the framework of the Nuclear Safety Research Division (NSRD) Post-Operational Phase (POP) for Tihange 2 and Doel 3.

- Maintenance Practices and Component Failure Rates:
  The ASME/ANS PRA standard [5] (in DA-B-2) groups data for parameter estimates based on operational mode, component type, and service conditions. IAEA SSG-3 (in 5.122) emphasizes addressing design and operational mode when selecting failure data. The impact of qualification on component failure rates is considered secondary to other factors such as component type and service conditions.

- Historical Data Sources:
  Generic data sources used historically in PSA studies do not support arguments for large differences in failure rates between safety-related and important-to-safety SSCs.

It should further be mentioned that a transition to FUNC was considered to not affect the structural capacity of the component and thus not affect its seismic fragility.

2.3. Human Reliability Analysis

During the post-operation phase (POP), operators have extended time frames for taking actions and recovering from errors, which is even more crucial during the POP than during at-power operation.

For tasks related to decay heat, the lower heat levels provide additional reaction time for operators compared to normal operation. Detailed deterministic studies were conducted to estimate decay heat evolution during the post-operational phase, considering factors such as the gradual permanent offloading of assemblies to spent fuel containers.

However, when it comes to human actions with time windows dependent on decay heat, existing quantifications often use an expansive time performance factor for most plant states. Despite this, the methodology was not updated to further reduce human error probabilities based on time windows. The argument is that predicting diminishing effects, due to exceptionally long- time windows, is challenging, and the applied human reliability analysis (HRA) method was not designed for such large time spans.

Instead, the focus shifted to accounting for additional recovery actions. Important human failure events (HFEs) were identified based on a Risk Increase Factor (RIF) greater than or equal to two. For these significant HFEs, the available system window time was assessed and compared to shift transition frequencies (including weekly schedule rotations) to determine if additional recoveries could be credited.

It should also be noted that procedures were updated for use during the post-operational phase and existing HEP values were also reviewed to account for changes in PSF. In particular the stress, ergonomics (labelling new system boundaries) and procedural availability factors had to be re-addressed.

2.4. Success Criteria

In the post-operational phase (POP), certain shared systems — supporting both the reactor and spent fuel pool — may have relaxed success criteria. Specifically, safety functions related to the reactor were revoked for some open-loop systems, freeing up capacity for spent fuel pool-related tasks.

For instance, consider the makeup systems. Original probabilistic safety assessment (PSA) models evaluated the need for reservoir refilling within the mission time scenarios. However, it was discovered that for some systems, reservoir makeup was no longer necessary. Similarly, in intermediate cooling systems, where some users were abandoned, a reduced number of pumps sufficed to meet the spent fuel pool's requirements and support systems during the POP.

Notably, differences existed between the two considered units based on their initial system design. For example, one unit had a system with each train containing two pumps, each operating at 50% capacity during normal operation. In contrast, the equivalent system in the other unit had only a single pump operating at 100% capacity per train. Demonstrably, the former system now meets the full requirements during the post-operational phase with just a single pump operating at 50% capacity.

2.5. System boundaries

A re-evaluation of potential flow diversion and line exclusion was performed based on updated individual component classification (SAFE/FUNC/ABAN). For newly defined system boundaries, it was assessed if isolation means would be such that they could be screened out in the PSA model for potential flow diversion. In Belgian PSA models, potential flow diversion paths are screened out based on of potential flow rate (<10% of nominal flow) or if two independent isolation means are available. If the newly identified boundaries could not be screened spurious operation and/or pre-accidental human errors of position, modifications were introduced into the model.

4. DEFENSE-IN-DEPTH ANALYSIS BASED ON PSA

The defense-in-depth approach was supported by probabilistic safety analysis (PSA) techniques, including Fault Tree Analysis and Bayesian Inference. These methods utilized data from existing PSA models for the unit. A dedicated evaluation was conducted to determine the expected frequency of occurrence of different Postulated Initiating Events (PIEs) specific to the units. The

list of considered PIEs was partially based on ANSI 57.2 [2] and IAEA SSG-15 [3], supplemented by expert judgment.

The reevaluation of Postulated Initiating Events (PIEs) categorization was based on their expected frequency of occurrence during plant conditions. The analysis specifically focused on the post-operational phase, where remaining fuel assemblies from the reactor still resided in the spent fuel pools while gradually being transferred to different storage facilities. The primary concern arose from the reduction of the nuclear island, as certain PIEs might change category. Consequently, the existing provisions in terms of number and type could become insufficient. This potential inadequacy could impact the design of the post-operational phase (POP) nuclear island and potentially lead to the rejection of a proposed POP configuration for the nuclear island.

Based on the ANSI/ANS-57.2 standard [1] and IAEA TECDOC 1791 [3], using expected frequency, the following plant condition (PC) categories are distinguished:

- PC I (normal operation) – annual frequency of occurrence > 1.
- PC II (normal operation) – annual frequency of occurrence $\geq 10^{-1}$.
- PC III (anticipated operational occurrences) – annual frequency of occurrence $< 10^{-1}$ and $\geq 10^{-2}$.
- PC IV or PC V (design basis accidents and/or design extension conditions without significant fuel.
- degradation ($< 10^{-4}$ and $> 10^{-6}$) – annual frequency of occurrence $< 10^{-2}$ and $> 10^{-6}$
- DEC (Design Extension Condition with significant fuel degradation) – annual frequency of occurrence $\leq 10^{-6}$.

The key findings and conclusions from this analysis are as follows:

- PIE Categorization:
    - Approximately half of the Postulated Initiating Events (PIEs) align with the categorization proposed in the ANSI N57.2 [1] standard.
    - For the remaining PIEs, the categorization for the considered units was higher (e.g., condition III instead of II) compared to the ANSI N57.2 [1] standard.
    - This discrepancy was observed both in the current configuration (Normal Operation) and across various potential post-operational phase (POP) configurations.
    - Notably, no PIEs were identified with higher occurrence probabilities in the units than specified by the ANSI N57.2 [1] standard.

- Increased Occurrence Probability in POP:
    - Four specific PIEs exhibit increased occurrence probabilities during the POP compared to the present configuration:
        - PIE 2.06: Loss of normal spent fuel cooling for up to eight hours. In certain potential configurations, this PIE shifted from a condition IV-V event (current plant configuration) to a condition III event due to reductions in the number of component cooling trains.
        - PIE 3.02: Loss of offsite power for up to 8 hours. Across all POP configurations, this PIE transitioned from a condition IV-V event (current plant configuration) to a condition III event. The reduction in external grid

connections played a significant role. In all considered POP configurations, only a single switchyard (150 kV) remained, replacing the initial two (380 kV and 150 kV). The modified switchyard arrangement impacted the frequency of switchyard-related LOOP events. Additionally, for one of the considered units, the frequency of grid-related LOOP events needed adjustment due to the connection of the two switchyards to different substations, affecting vulnerability to partial loss of the national grid.

- PIE 3.09b: Drop of the spent fuel cask from controlled normal height. In all POP configurations, this PIE shifted from a Design Extension Condition (DEC) to a condition IV-V event. The reassessment considered manipulations in the pools, accounting for planned activities (e.g., filling of containers) during the post-operational phase.
- PIE 4.04b: Drop of the spent fuel cask from maximum achievable height, following similar reasons as the previously mentioned PIE.

No PIEs were found, for the considered configuration, to drop their expected frequency by such magnitude that a decrease in plant condition could be warranted. However, insights were gained:

- PIE 2.05- Single failure in the electrical or control system was found to reduction in support system trains and associated control logic decreasing the frequency for spurious operations.
- PIE 2.10 Failure of any single active component to perform its intended function upon demand. Operation of remaining support systems, originally shared with the reactor is simplified reducing expected frequencies of re-alignments, system configuration changes, etc.

For each of the listed Postulated Initiating Events, categorized by plant conditions, and for each of the considered scenarios, a compilation of provisions has been identified. These provisions are retained in the existing Safety Function Performance Assessment (SFP PSA) models and are present in relevant PSA model cut sets. Additionally, some provisions are referred to in PSA screening analyses, even if they are not explicitly modeled in the PSA. In this context, a provision refers to measures implemented in design and operation, such as inherent plant characteristics, safety margins, system design features, and operational measures [4]. These measures contribute to the performance of safety functions aimed at preventing specific mechanisms from occurring.

Identified provisions were further subdivided in:

- Level 1 – Prevention of abnormal operation and failures, i.e., provisions preventing of the PIE from occurring.
- Level 2 – Control of abnormal operation and detection of failures, i.e., normal operation practices and systems able to prevent the situation from escalating.
- Level 3 – Provisions designed to protect the unit against design basis accidents.
- Level 4 – Provisions designed to protect the unit during severe accidental conditions.
- Level 5 – Provisions to mitigate the consequences of significant releases.

For each considered plant configuration, a matrix was established to assess the impact of the configuration on the available plant provisions in light of the updated plant condition.

Simultaneously, a review of deterministic safety studies was initiated for the PIEs and crediting systems affected by the plant configuration. The insights from this review were then combined with the information obtained from the earlier analysis to arrive at the defense-in-depth conclusion.

5. PSA MODELLING ASPECTS FOR LTE

For the LTE risk-informed approach, applied on the youngest units Tihange Unit 3 and Doel Unit 4, a number of design upgrade candidates had been identified based on deterministic and probabilistic (dominant sequences) inputs. For those upgrades that could be evaluated using level 1 PSA a risk analysis was performed. The quantification of Design Upgrade Candidates (DUC) was not limited to individual upgrades but rather combinations of DUCs were considered (i.e., cumulative impact on CDF). This as it was found that, due to dependencies, non-negligible diminishing returns between the considered candidates where observed. An example of such dependencies that had to be explicitly modelled pertained to the installation of an ATWS mitigation signal and replacement of the pressurizer safety valves. While a direct link between the two modifications is perhaps not evident as the ATWS scenario consists of one of the most severe challenges to the safety valves in terms of potential cycling and water actuation solely considering the two modifications in isolation could hamper the judgment of the safety significance of both modifications.

It was the objective of the analysis to confirm that the final proposed design upgrades (or PDUs) are adequate and verify that non retained DUCs do not represent large missed opportunities in risk-reduction. This is in order to facilitate decision making in a manner that corresponds to the actual risk presented ‘as-operated’, so called ‘risk-informed approach’ and to complement deterministic considerations that form the backbone of the selection. To meet this objective the hypotheses and data of the existing PSA model had to be reviewed and newly available information introduced in the modelling to obtain a degree of ‘conservative realism’ that is suitable for such activities. Furthermore, as details with respect to the implementation of particular DUC had not been fixed different alternatives have been modelled.

It can finally also be noted that by integrating PSA at early design stages alternative suggestions and points of caution could be raised related to procedures and interplay that would otherwise normally not be available at such early stages in the design.

6. CONCLUSIONS – LESSONS LEARNED

By combining the efforts of deterministic safety studies, defense-in-depth analysis and PSA the minimum required nuclear island was able to be defined. Table I depicts a high-level overview of the main systems for the identified minimal required nuclear island configuration for the Doel 3 unit (non-exhaustive list). Similarly, using PSA valuable insights on the risk significance of potential design upgrades was obtained in preparation for the LTE for the Doel Unit 4 and Tihange Unit 3. Interactions between different investigated upgrades could be identified.

Open and frequent discussions with the safety authorities and their technical support office were required order to reach a timely agreement on both the minimum required shutdown configurations as in establishing a list a proposed design upgrades for the units retained for long term operation.

Table I. Minimum Nuclear Island

System	POP-3
Component Cooling System	FUNC A: 2 trains (2nd train in standby)
	ABAN: 1 train
Safety Grade Degassed Demineralized Water System (Pool Make-Up)	SAFE: 2 trains
First Level Diesels	SAFE: 1 train (shared diesel with operational unit)
	FUNC A: 1 train
	ABAN: 2 trains
Fire Extinguishing System (Potential Make-up Source)	FUNC A: 3 trains
Emergency Diesels	SAFE: 2 trains
	ABAN: 1 train
Emergency Cooling System	SAFE: 2 trains
	ABAN: 1 train
Non-Safety grade Demineralized Water (Pool Make-Up)	FUNC A
Pool Loops	SAFE: 2 trains
Safety Grade Service Water	FUNC A: 2 trains (2nd train in standby)
	ABAN: 1 train

These projects were the first application of an integrated safety approach on such scale within Belgium. The projects were performed by a large integrated team containing deterministic and probabilistic safety assessment experts, operational staff, maintenance staff, etc. which was deemed required for success.

While regulation remains in 'deterministic first' within Belgium, the risk insights provided by PSA modelling was positively evaluated by the operator and authorities alike.

REFERENCES

1. ANSI/ANS-57.2-1983, Design Requirements For Light Water Reactor Spent Fuel Storage Facilities At Nuclear Power Plants
2. IAEA Safety Standards Series No. SSG-15 Storage of Spent Nuclear Fuel
3. IAEA TECDOC 1791 Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants
4. IAEA Nuclear Safety and Security Glossary
5. ASME/ANS RA-S-2008 Standard for Level l/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications
6. Application of Probabilistic Safety Assessment Within an Integrated Safety Approach for Re-Design of the Nuclear Island During Post-Operational Phase, Filip Van Opstal & Federico Agosti, 18th International Probabilistic Safety Assessment and Analysis (PSA 2023), Pages 801-813