Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27883-cd

Development of a Full Scope External Hazard PSA for Gösgen NPP

Gerben Dirksen

Framatome GmbH, Germany. E-mail: gerben.dirksen@framatome.com

Dusko Kancev

Gösgen Nuclear Power Plant, Switzerland. E-mail: DKancev@kkg.ch

In the second phase of the PSASpectrum project, a full scope internal flooding and external hazard PSA was developed for Gösgen nuclear power plant. The PSA encompassed external hazard screening based on the list of potential hazards from the ASAMPSA_E project. Relevant hazards including earthquake, external flooding, airplane crash, strong wind and tornado as well as local man-made hazards and hazards leading to unavailability of the water intake have been evaluated. In addition, relevant combinations of hazards were reviewed.

For the screened in-hazards, detailed analysis was performed for all plant operating states. The integration of fragilities for earthquake, wind and tornado was performed using the RiskSpectrum® ModelBuilder software. In addition, the human reliability analysis methodology developed in phase 1 of PSASpectrum (internal events) was extended to include effects relevant to internal flooding and external hazards.

The hazard analysis was then embedded in the existing full scope internal events model, quantifying the results for Level 1 PSA and Level 2 PSA in a fully coupled model. To achieve acceptable calculation time in combination with accurate results, the newest features of RiskSpectrum® PSA such as BDD quantification, mutual exclusivity between basic events and conditional quantification were used.

The development of the full scope PSA for Gösgen shows that with modern computing power, modeling a fully coupled, traceable PSA for a nuclear power plant down to the component level is feasible and can provide deep insights in the risk profile of the plant and its systems, structures and components.

Keywords: Probabilistic Safety Analysis, External Hazards, Seismic.

1. Introduction

In the PSASpectrum project, a new full scope probabilistic safety analysis (PSA) has been developed for Gösgen Nuclear Power Plant in accordance with regulatory guidelines ENSI-A05 and ENSI-A06. The project consisted of two phases:

(i) Internal Events
(ii) Internal Hazards and External Events

The first phase was finalized at the end of 2023, the second phase was conducted in 2024 and 2025.

In internal events modeling, innovative methods using RiskSpectrum® ModelBuilder (RSMB) for system modeling, event tree modeling using Event Sequence Diagrams (ESD), and PSA-specific failure mode and effect analysis (FMEA) were used to create a coupled, fully traceable Level 1 and Level 2 PSA model.

For details on the use of RSMB, refer to (Dirksen et al., 2022) and (Kancev et al., 2022). For details on the ESD, refer to (Hausherr and Kancev 2024).

2. Modeling of external hazards

The development of the full scope PSA model for external hazards consists of the following steps:

(i) External hazard screening analysis
(ii) Development of hazard master event trees
(iii) Development of special for emergency situations
(iv) Hazard-specific human reliability evaluation
(v) Quantification of the integrated Level 1 – Level 2 model for external hazards

The five steps will be described in more detail in the following chapters.

2.1. *External hazard screening analysis*

For the external hazard screening, the hazard list from ASAMPSA_E (Decker 2017) was chosen, as this list covers all hazards required by regulatory guideline ENSI-A05. The screening process was performed in several steps.

First, a pre-screening of the hazard list was performed, screening out hazards that are not relevant to the site or can be screened out on general considerations.

Then, a detailed site-specific and design-specific screening was performed, leaving the following list of potential hazards:

- Earthquake
- External flooding
- Strong wind and Tornado
- Tornado
- Loss of Ultimate Heat Sink (LUHS)
- Man-made hazards (explosion, chemical release)

The hazard frequency was calculated in different ways:

For earthquake, strong wind, tornado, and external flooding (events that cannot be screened out in accordance with ENSI-A05), the hazard was divided into several bins with different strength.

For airplane crash, the hazard was subdivided into small aircraft, five types of commercial aircraft, and military aircraft.

The frequency of other man-made hazards was calculated based on a covering scenario with a fixed frequency. Finally, as many different and diverse hazards can lead to LUHS, the frequency of the hazard was derived directly from plant operating experience.

2.1.1. *Combinations of hazards*

A dedicated report considers the combinations of hazards identified in the ASAMPSA_E project. In addition, in accordance with ENSI-A05, the combination of multiple hazards caused by either harsh winter conditions or extreme summer conditions were analyzed.

All combinations of hazards could be screened out.

2.2. *Development of hazard master event trees*

In RiskSpectrum® PSA, event trees can be coupled while inheriting the boundary condition sets through coupled event trees. Making maximum use of this feature, for each hazard a master event tree was created.

In the master event tree, it is decided which internal event transient is induced by the external hazard.

The master event tree for seismic events is shown in Figure 1. The event tree is designed in such a way that more severe events are queried before less severe events. The less severe events are then considered also inside the fault tree model for the more severe events.

After the initiating event, first it is queried if the fragility of the reactor building is exceeded (leading directly to large release – sequence 14). Next, sequences leading directly to core damage are considered. These are:

- Failure of critical components (sequence 13)
- LOCA outside containment in combination with loss of the MCR (sequence 12)

The other events queried in the event tree are, in order from severe to less severe:

- LOCA outside containment
- LOCA inside containment
- Loss of main control room
- Secondary side break
- Loss of off-site power

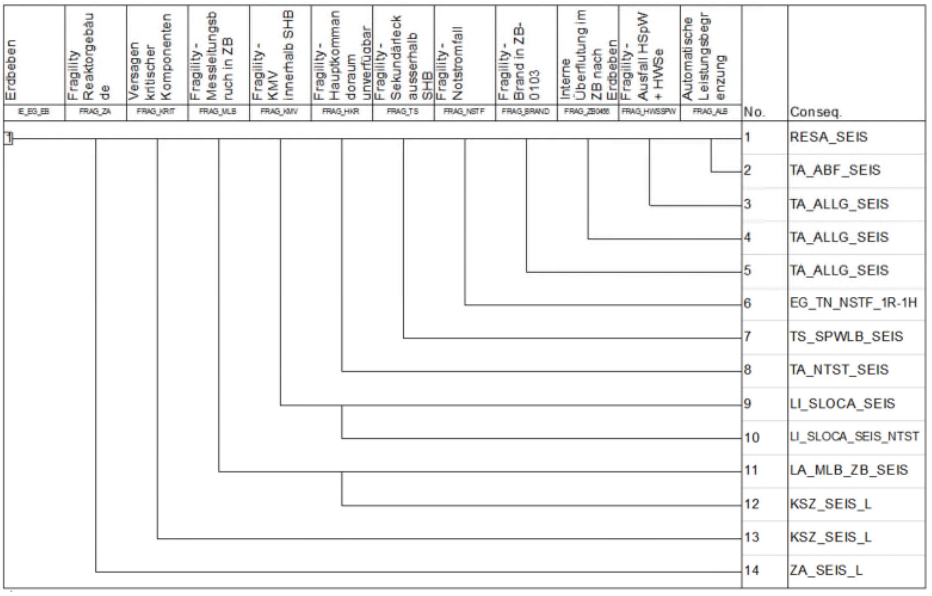

Fig. 1. Master Event Tree for Airplane Crash

- Seismically induced fire
- Seismically induced flooding
- Transient causing reactor trip (assumed loss of main feedwater and main heat sink)
- Seismically induced reactor trip

After the master event tree, subsequent event trees are developed based on the existing internal events event trees. For some cases however, new event trees were developed, as detailed in the next section.

2.3. *Development of special ESD for emergency situations*

As some scenarios after internal and external hazards are not covered by internal events, additional event trees need to be developed to cover these cases.

The following scenarios were modeled with specific event trees, but using the existing ESD from internal events:

- Total Station Blackout – defined as loss of off-site power, and loss of both the emergency diesel generators and ultimate emergency diesel generators
- Loss of the first and second water intake

A dedicated ESD was however created for the special emergency scenario, which is defined as a loss of the main control room, e.g. plant shutdown from the remote shutdown station (RSS).

The reason for the dedicated ESD is the availability of a dedicated chapter in the operating manual for the plant shutdown from the RSS.

The structure of the ESD again followed the methodology outlined in (Hausherr, 2024).

2.4. *Hazard-specific human reliability analysis*

In accordance with ENSI-A05, the human reliability analysis for hazards considers the potential for:

(i) Increased stress and confusion,
(ii) Reduced availability of personnel,
(iii) Limited accessibility and habitability of relevant areas,
(iv) Failed or erroneous instrument indications,
(v) Additional workload on personnel,
(vi) Additional difficulties in the detection/diagnosis of certain hazards
(vii) Limited accessibility to areas of the plant.

This was ensured by the following methodology:

First, for each hazard, the feasibility of the relevant operator actions was evaluated in a conservative way. For example, it was assumed that human actions on the plant area are not possible during the duration of a strong wind event.

Then, the nature of the hazard was considered: Some hazards like external flooding and strong wind are "expected" hazards, in the sense that the plant staff can prepare for the hazard. Other hazards like airplane crash, tornado and earthquake are "sudden" hazards and do not allow pre-hazard preparation. On the other hand, the expected hazards often have a longer duration, during which the severe conditions stay in effect.

Based on the nature of the hazard, the time available after the initiating event and the location of the operator action, hazard-specific performance shaping factors were applied to the human error probabilities for relevant operator actions.

For the specific action steam generator feed using the electrical special emergency feedwater pump, which is only relevant for very specific hazards, a hazard-specific human error probability evaluation was performed.

2.4.1. *Human reliability for seismic events*

A seismic event is a special type of "sudden" hazard, as it affects the whole site and even protected areas such as the main control room directly. Therefore, to evaluate human reliability after a seismic event, so-called seismic shock models have been developed. The regulatory guide ENSI-A05 contains such a seismic shock model, however the suggested model has the disadvantage, that the resulting human error probability is practically independent of the complexity of the human action.

A specific seismic shock model was therefore developed, which is described in detail in (Kancev 2026).

2.4.2. *Dependency analysis for hazard HRA*

Dependency analysis is an important topic when evaluating human reliability. In the development of the Gösgen PSA model, a dependency decision tree for human actions was developed. This decision tree was extended for the use in hazard HRA. The dependencies were then integrated into the RiskSpectrum® PSA model.

Particularly of interest for the external event PSA was the evaluation for "expected" hazards. If an extreme event such as external flooding or strong wind is expected, it can be beneficial to prepare against this. Such events were considered as type B human actions (human actions that, if failed, lead to an initiating event) In the case of Gösgen, useful actions to prepare against external flooding are:

- Erecting a dedicated barrier protecting the essential service water building ZM02
- Relocate the mobile diesel generator in preparation of steam generator feed with electrical special emergency feedwater pump

2.5. *Quantification of the integrated Level 1 – Level 2 model for external hazards*

The Gösgen PSA is an integrated PSA, therefore Level 1 PSA and Level 2 PSA are quantified in a fully integrated way.

For each of the hazards, analysis cases are created quantifying core damage, large release, and all release categories.

For most hazards, quantification can be performed like internal events PSA, that is using logical event tree success (assuming the success path has probability 1.0) to calculate core damage.

However, especially the seismic PSA requires special treatment, as there are two issues:

- Sequences in the master event tree are mutually exclusive
- Large probabilities occur in practically all event trees

2.5.1. *Quantification of the seismic master event tree*

In the seismic PSA, the hazard curve is divided into several seismic bins with different peak ground acceleration (PGA). The main contributing bins for the Gösgen PSA are:

- Bin SEIS6: 0.6 g < PGA < 0.8 g
- Bin SEIS7: 0.8 g < PGA < 1.1 g
- Bin SEIS8: 1.1 g < PGA < 1.7 g

Fig. 2 shows the transients that are induced by the seismic events 6 through 8 and their relative frequency in comparison with the initiating event frequency. The events analyzed are:

- Loss of off-site power (LOOP)
- Secondary break (e.g. loss of turbine hall)
- Special emergency (loss of main control room)
- Loss of coolant accident (LOCA)
- Interfacing system LOCA
- Direct core damage (e.g. failure of primary circuit)
- Direct large release (e.g. failure of reactor building)

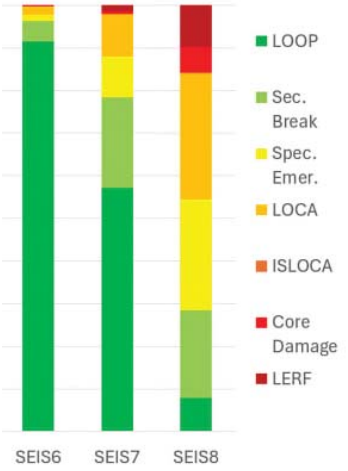

Fig. 2. Induced Initiating Events, Seismic Bins 6 – 8

It is observed that the incidence probabilities of the induced events cannot be considered "small" in the PSA sense. Therefore, to not overestimate the occurrence of the less severe events, the function events in the hazard master event tree are treated calculated using "logical and simple quantitative" settings, that is, the success path is calculated directly as one minus the failure probability.

2.5.2. *Quantification of the seismic core damage frequency*

Calculating the core damage frequency using minimal cut sets and the min cut upper bound (MCUB) approximation is reasonable when dealing with small probabilities, but in seismic PSA, failure probabilities are by nature high, as beyond design earthquakes are analyzed.

For this reason, when using MCUB even in combination with "logical and simple quantitative" approximation, as outlined in the previous section, will lead to conditional core damage probabilities (CCDP) greater than 1 for some initiators.

RiskSpectrum® PSA however offers a solution for that problem. Using the MCS BDD algorithm, the result of an existing minimal cut set list is taken, and an exact solution for the top cut sets is calculated. The remaining cut sets are then added using MCUB.

With this approach, it was found that when applying a sufficient amount of BDD nodes (in the case of the Gösgen PSA, 100 million nodes were required), in fact a CCDP of less than 1 or close to 1 was found for each initiator.

2.6. *PSA risk evaluation*

To be able to benefit from PSA as a tool for minimizing the risk or to perform applications such as risk-informed decision making, the full scope of initiating events, including all internal and external hazards needs to be considered.

The total risk level for the Gösgen nuclear power plant, with core damage frequency (CDF) well below 1E-05 / year, is very low. In fact, the main contribution to CDF with approximately 2E-06 / year comes from seismic events. The main contributing seismic initiators have a PGA > 0.6 g, well above the deterministic seismic design of the plant and very rare events considering the hazard curve. It should be recalled that the contribution from seismic events with very low annual probability of exceedance (less

than 1E-5 / yr) is subject to a high level of uncertainty. Correspondingly, the question on how to deal with their contribution in the overall assessment of risk is a matter of debate in the nuclear industry, see McSweeney (2021) and Luzoir et al. (2023).

A disadvantage of such a result for risk-informed decision making, is that non-seismic plant improvements do not show a significant risk increase, even though they are significant when not accounting for earthquakes.

2.7. *Main risk insights*

The main result of new PSA for Gösgen shows that many planned, ongoing and completed safety improvements in the plant are in fact beneficial for the risk level.

This is especially true for the following completed improvements:

- Automatic seismic shutdown
- Passive isolation valves in measurement lines
- Automatic fast secondary cooldown after 30 minutes in LOCA conditions

In addition, the PSA confirmed the following ongoing modifications:

- Seismic refitting of cable trays in reactor building annulus
- Operating manual modification to isolate component cooling system break before draining annulus bunkered area (avoid flooding of reactor building annulus)

Nevertheless, the most interesting risk reduction measure was found that the plant has the means to effectively prepare against an imminent external flooding event, by setting up the mobile diesel generator unit where it could be used in an optimal way.

3. Conclusions and future work

The implementation of the risk monitoring software RiskSpectrum® RiskWatcher using the new PSA model is still ongoing. The PSA model will be used for risk-informed applications such as optimization of the emergency operating procedures (EOPs) and updated for use in the upcoming periodic safety review.

With this new, modern and up-to-date PSA, Gösgen NPP can show its high safety level and prepare for long term operation.

Acknowledgement

Many thanks to Anders Olsson and Xuhong He for their expert insights during the development of the Gösgen PSA model.

References

Decker, K., Brinkman, H (2017). List of external hazards to be considered in ASAMPSA_E, ASAMPSA_E/WP21/D21.1/2017-41

Dirksen, G. et al. (2022). Creating a digital twin reliability model using RiskSpectrum® ModelBuilder. Proceedings of the 32nd European Safety and Reliability Conference

Hausherr, R., Kancev, D. (2024). Development of Specific PSA-tailored ESDs: A real-case industrial-scale implementation. 17th International Conference on Probabilistic Safety Assessment and Management

Kancev, D., Dirksen, G., Hausherr, R. (2022). Development of a new plant-specific, full-scope industrial-scale L1/L2 PSA-model with the application of the new RiskSpectrum® ModelBuilder Tool. Proceedings of Probabilistic Safety Assessment and Management PSAM 16

Kancev, D., Dirksen, G. (2026). Seismic-HRA Methods Implementation in a Realistic-NPP Model: Comparative Analysis on a Plant-Level Risk Contribution, Proceedings of the 36th European Safety and Reliability Conference

Lezoir, C. et al. (2023), EDF Hierarchization Process for PSA Insights valuing Strength of Knowledge

McSweeney, L. (2021), Risk Applications of Extreme Seismic Hazard Modeling; PSA topical meeting 2021