Risk Assessment of Outage Plans at Ringhals NPP Using RiskWatcher

Anna Bjereld
Ringhals, Väröbacka, Sweden

Abstract: Ringhals units 3 and 4 are 3-loop Westinghouse PWRs from the 1980s with PSA models covering L1 and L2, considering internal events and external hazards, internal fire and flooding during power operation and shutdown. PSA models for the spent fuel pools are under development.

In 2018, the risk monitor RiskWatcher was implemented for Ringhals 3 and 4 and is used for assessment of outage plans in order to identify potential nuclear risks and verify that risks are minimized. Risk assessment is performed based on outage plans 120 days and 30 days ahead of outage. A risk follow-up is performed after outage. The risk assessment calculates CDF using RiskWatcher with input from the outage plan as well as work orders for equipment out of service.

Ringhals' contribution to PSAM is a presentation of the development of a RiskWatcher model and application of this model for risk assessment of outage plans. This paper also discusses some problems and challenges related to risk assessment over time.

Keywords: Risk monitor, RiskWatcher, outage, shutdown

1. INTRODUCTION

The RiskWatcher models for Ringhals units 3 and 4 were developed by Lloyd's register in 2018. The purpose was to get a tool to improve outage planning since almost all maintenance is performed during shutdown due to Technical Specifications requirements in accordance with Swedish regulations.

Ringhals units 3 and 4 are 3-loop Westinghouse PWRs from the 1980s. PSA for Ringhals has been performed since the 1980's in different stages with now living PSA L1 and L2 models that strive to be state-of-the-art covering internal events and external hazards, fire and flooding during power operation and shutdown. PSA models for the spent fuel pools are under development.

2. TERMINOLOGY

PIS	Process Information System
POS	Plant Operating State
RIDM	Risk-Informed Decision Making
RIF	Risk Increase Factor (compared to normal power operation)
SPSA	Shutdown PSA
WCM	Work Clearance Module in Ringhals business system, SAP
baseline PSA model	the PSA model for power operation and shutdown presented in the Safety Analysis Report representing risks during one reactor year
application PSA model	the PSA model for power operation and shutdown used in RiskWatcher representing CDF at a given plant configuration and POS

3. CONVERSION OF BASELINE PSA MODEL INTO APPLICATION PSA MODEL

The application PSA model for use in RiskWatcher is integrated in the baseline PSA model in RiskSpectrum, meaning that they share some fault trees and event trees. Before conversion of the PSA model, adjustments to remove asymmetrical assumptions about trains in operation in the baseline PSA model were made.

3.1. System Configurations

System configurations enable the selection of which equipment is operating, ready for operation or unavailable. An example of this is which steam generator is used for cooling during hot shutdown. Another example is the possibility to select which train in a system is in stand-by.

System configurations are defined using boundary condition sets and related attributes in RiskSpectrum. The boundary condition sets include a number of house events that can be set be TRUE or FALSE and hereby connect or disconnect fault tree branches corresponding to different system configurations.

In total there are 13 system configuration groups in the Ringhals application PSA model, including availability of electrical sub-divisions, alignment of steam generators, RHR, SI, CC and salt water pumps in standby.

In addition to the system configurations modelled, heavy lift has also been modelled using system configurations. The consideration of lift of reactor head is represented when the system configuration is set. When this event is set, the frequency event of drop of reactor head is included in the analysis. The consideration of lift of heavy equipment in the turbine hall that may damage the salt water system is also considered. When this event is set, the frequency event of drop of heavy load in the turbine hall is included in the analysis (currently only possible in cold shutdown before refueling).

3.2. Plant Operating States

The application PSA model covers full power operation and shutdown, plant operating states:

Power Operation	POS 1
Startup	POS 2
Hot Standby	POS 3
Hot Shutdown	POS 4:1 (before refueling, 1 RHR pump operating)
	POS 4:2 (before refueling, 2 RHR pumps operating)
	POS 4:3 (after refueling)
Cold Shutdown	POS 5:1 (before refueling)
	POS 5:2 (after refueling)
Static Shutdown	POS 5*:1 (before refueling)
	POS 5*:2 (after refueling)

Midloop operation is generally not performed at Ringhals units 3 and 4 and thus not modelled. Refueling and Unloaded Core are not modelled since no identified events lead to core damage within the PSA timeframe of 24 hours. PSA models for the spent fuel pool with consequences other than core damage are under development and not yet included in the application PSA model.

POSs are defined using boundary condition sets in RiskSpectrum. When the plant is in a specific POS, the initiating events relevant for this POS will be set to normal by the boundary condition set and the initiating events relevant for all other POSs will be set to FALSE.

3.3. Component and Basic Event Mapping

In RiskWatcher, more than 1,000 components that are represented in the application PSA model can be selected by a user to be taken out of service. The relation between basic events and components is linked with attributes for selected basic events that shall be set to TRUE to represent component unavailability. Some components have more than one failure mode in the PSA model (like the PORV that can fail to open or fail to close). To define which basic event that most adequately corresponds to component unavailability a comprehensive mapping of components to basic events has been performed. The basic events where PORVs fail to open and safety valves fail to open are selected to represent unavailability. For micro circuit breakers, the whole cabinet is conservatively assumed to fail. Some components are linked to several basic events.

3.4. Initiating Event Scaling

The initiating events in the baseline SPSA model are scaled to consider that the time in each POS is only a fraction of an operational year. For example, the initiating events in cold shutdown in the baseline PSA are weighted down to reflect that the time fraction in that POS is only 0.7% of the year. In a risk monitor application, the frequencies for initiating events in cold shutdown are only calculated when the plant is in that POS and no weighting is applied.

When developing the application PSA model, re-scaling of frequencies in the baseline SPSA model has been performed to adjust for the considered time fraction. The power operation initiating events have not been rescaled which is an acceptable simplification due to the low impact. The re-scaling is based on the assumption that the initiating event frequency is proportional to the time spent in the POS:

$$f_{RW} = f_{baseline} \cdot 8760/t_{POSx}$$

where

f_{RW} = instant rate of occurrence of initiator in specific POS (/year) in the application PSA model

$f_{baseline}$ = "per calendar year" frequency of occurrence of initiator in POS (/year) in the baseline PSA model

t_{POSx} = duration of POS (hours in POS/year) in the baseline PSA model

The approach is suitable for initiating events which may occur randomly at any time in a POS. As discussed further in section 5.1, demand-based frequencies where initiating event frequencies are not proportional to POS durations are not treated differently with the exception of drop of heavy load frequency.

3.5. Analysis Case Modelling

The application PSA model only contains one consequence analysis case for core damage. This is due to a restriction in RiskWatcher that each analysis case should contain all the information required to resolve that consequence. That is, if core damage is studied then it must be possible to run core damage as one analysis case. This has caused a significant restructuring of the analysis cases in the Ringhals 3 and 4 PSA models.

4. RISKWATCHER ASSESSMENT OF RINGHALS 4 OUTAGE

From 2018 Ringhals uses RiskWatcher to minimize risks in the outage plans and verify that the risk levels during outage were acceptable. During 2018, the outage plan for Ringhals 4 was assessed 120 days before outage and 30 days before outage with a beta-version of RiskWatcher 2.1. The actual outage risk will be assessed in the next risk follow-up in the end of the year.

4.1. Input Data in Planning

Input data with time points for POS entries and heavy lifts were gathered from the time schedule in Primavera. System configurations were not known at the time of the assessment and therefore the same configurations as in the baseline PSA model were assumed, except for all power sub-divisions which were assumed to be available when no work was going on. Standard isolations and work orders together with scheduled time-points stored in WCM (Work Clearance Module) in Ringhals business system, SAP, were used to identify equipment out of service. Import and mapping to components in RiskWatcher was achieved with a beta-version of the import tool RiskWatcher Connector.

4.2. Input Data in Risk Follow-Up

Risk follow-up after the Ringhals 4 outage in 2019 has not yet been finalized. Input data is expected to be retrieved in a similar way as for the Ringhals 4 outage in 2018 and Ringhals 3 outage in 2019.

Input data about time points for POS entries and heavy lifts will be gathered from AutoLog. System configurations stored in PIS (Process Information System) will also be gathered from AutoLog due to the AutoLog PIS-import function. Standard isolations and work orders together with actual time-points stored in WCM in SAP will be used to identify equipment out of service. Import and mapping to components in RiskWatcher will be achieved with the import tool RiskWatcher Connector.

4.3. Application Method

The following risk curves are calculated with RiskWatcher:

1. Basic risk level for the outage without component unavailability (”Mode-Only”)
2. Risk level for the outage including planned outage activities and heavy lifts, conservative
3. Risk level for the outage including planned outage activities and heavy lifts, adjusted

No. 1 is calculated as a reference level. No. 2 is calculated to represent all input data. Now, work orders include a listing of affected equipment for the activity and all listed equipment is conservatively set to out of service in RiskWatcher. In reality, all listed equipment will not be unavailable. For instance, a valve can be listed because flow through it shall be verified. No. 3 is calculated where adjustments have been made, for instance that only unavailable equipment is modelled as out of service. No. 3 is calculated after discussion with planners.

4.4. Comparison with Safety Criteria

Risk indicators are defined as shown in Table 1. They are derived from Ringhals safety goals and used in a similar way as in risk follow-up. Risk Increase Factor is calculated related to the risk level for normal power operation. Accumulated risk is calculated in relation to Mode-Only risk. The same criteria are used for all POSs, not considering that uncertainties and assumptions might vary between POSs.

Table 1. Risk indicators for instant and aggregated risk

Indicator	Green (normal)	Yellow (acceptable)	Red (not acceptable)
Risk Increase Factor	<10	10-100	>100
Accumulated Risk (ΔRISK)	<10%	10-100%	>100%

4.5. Results and Discussion

RiskWatcher results for the assessment 120 days before outage (T-120) and 30 days before outage (T-30) planned between August 28th and September 28th are shown in Figure 1 and Figure 2 below.

Figure 1. R4 Outage 2019, T-120

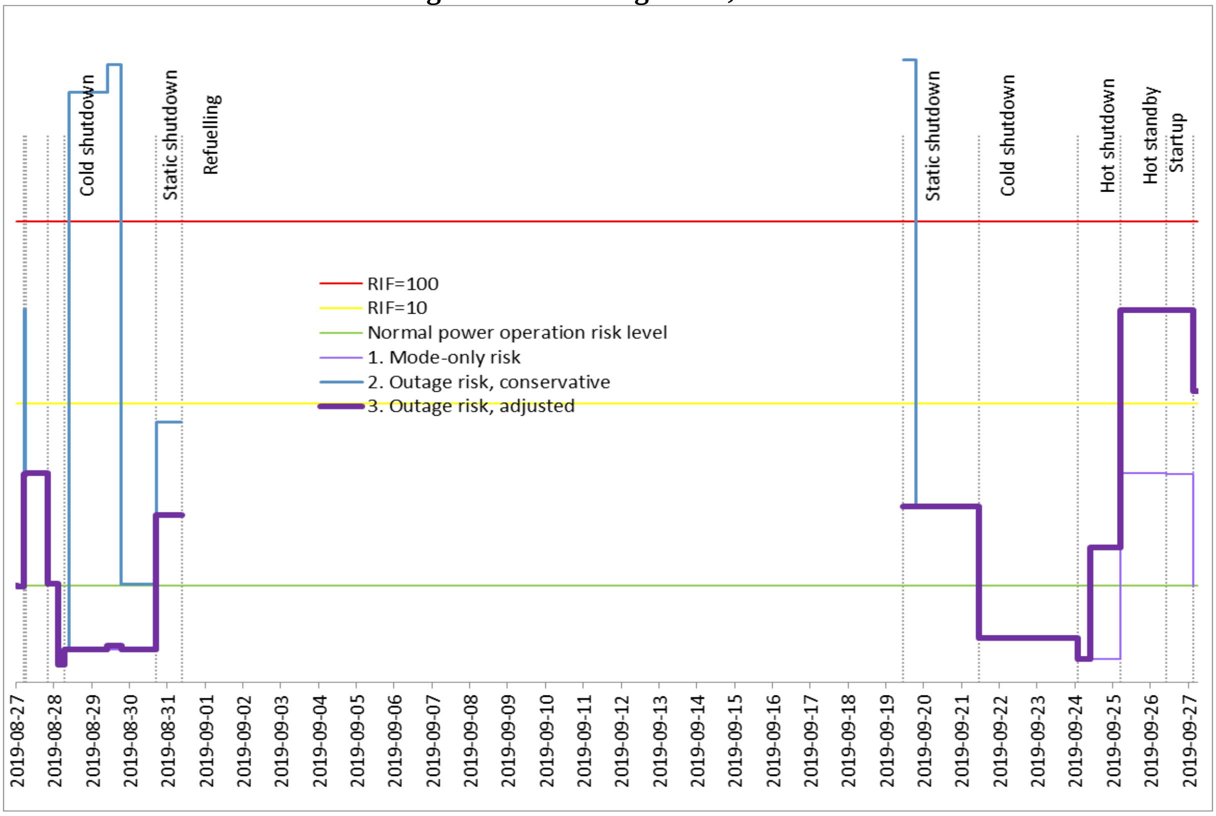
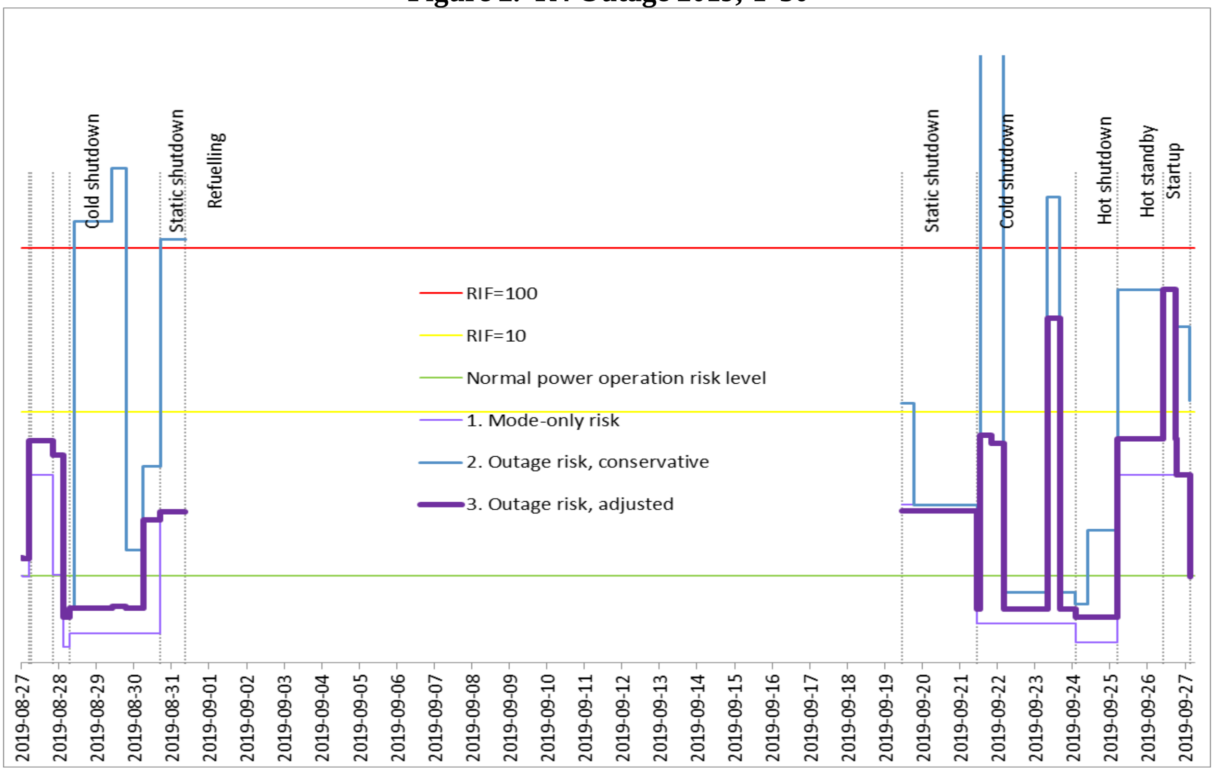


Figure 2. R4 Outage 2019, T-30



As one can see, the assessment 30 days before outage is more detailed mainly due to more work orders in WCM. Risk curve No. 2, the conservatively modelled risk level for the outage, highly overestimates the risk. Adjustments are therefore necessary even though they are time-consuming.

The assessment at T-120 adjustments to curve No. 3 include to correct that some listed equipment will not be taken out of service and that a cabinet will still be operable when demounting selected cables. Additional T-30 adjustments include that activities on the main steam relief valves are made on opened valves and they can thus be assumed available for steam discharge. Some tests on redundant RHR trains are planned at the same time in Primavera but will be performed in sequence which is adjusted in the model. System configuration is adjusted in order to avoid operable equipment to be modelled in standby when outage activities are performed on the redundant equipment.

According to the results, the highest risk is in low power operation and down to hot standby (since certain actions to shut down the reactor contribute with a higher risk) and in static shutdown (since this is a vulnerable state where the steam generators cannot be used for cooling). The time in static shutdown is limited and the planned outage activities do not contribute with unacceptable risk increase, thus the risk level is acceptable. No risk levels are calculated during refueling and unloaded core.

The following planned activities were highlighted due to their significant contribution to the calculated risk level (conservative or adjusted):

- A project with activities on instrument air system means unavailable air compressors and other equipment during the whole outage. The real risk is probably lower than the calculated risk since instrument air should be taken from Ringhals 3 in the meanwhile and backup diesels were brought (adjusted risk not quantified)
- Steam generator 2 out of service in cold shutdown (“green” risk)
- Tests on RHR trains in cold shutdown (“green” risk if performed in sequence)
- Tests on SI in cold shutdown (“yellow” risk if all valves are unavailable at the same time)
- High Δ-risk for adjustment of steam-driven AFW pump overspeed actuation (a just-in-case job, “yellow” risk if performed)
- Demounting of cables from a cabinet important to safety (adjusted risk not quantified)

5. REPRESENTATIVITY OF THE APPLICATION PSA MODEL FOR RIDM

The baseline PSA model gives a good representation of the plant risk profile during an average reactor year. It can be used to identify plant weaknesses or verify that risks are smoothly distributed. But how can one be certain that a straight-forward translation of the baseline PSA model into a time-dependent application model is representative and can be used for risk-informed decision making? In order to make results for different POSs comparable and reflect plant risk adequately over time, the resolution of the application PSA model might need to be higher than of the baseline PSA model. Findings on this based on Ringhals experience are given in the following sections.

5.1. Time-Based and Demand-Based Frequencies

Time-based and demand-based frequencies for initiating events can be treated differently in the application PSA model for a higher resolution. Whereas loss of offsite grid can be considered quite constant over time (the frequency is time-based), drop of heavy load can only occur when performing a lift and maintenance-induced LOCA might be limited in time to when a valve is operated (demand-based frequencies). Activities with demand-based frequencies can be modelled using environmental factors or system alignments in RiskWatcher.

One example from Ringhals where the resolution for demand-based frequencies can be improved in the application PSA model is the initiating event overpressure. The overpressure frequency in the baseline PSA model is based on an aggregation of manual actions that are performed once during an outage and system malfunctions that can occur at any time, scaled to the length of the POS for an average outage. This is appropriate when calculating risk contribution from an average outage. For a specific shutdown the time in the POS might be longer or shorter. The time for the manual actions is limited to the time of the activity or the actions might not be performed at all. Thus the application PSA model does not reflect how risk varies over time. In addition, the accumulated risk in the POS might be over- or underestimated if the time in the POS is different than during an average outage.

5.2. Screening Criteria

Screening criteria in the baseline PSA model for shutdown might exclude events with high instantaneous risk that are relevant in the application PSA model. The screening of events in the baseline PSA model for shutdown might need to be revised for the application PSA model.

For instance, an initiating event with a time-dependent yearly frequency of 1E-8 might be included in the power operation model but has been screened out from the shutdown PSA using a scaling factor representing the short time in the POS. Considering the frequency per hour instead of the full year frequency, the event is equally probable during an hour in power operation as in shutdown. The screening might thus lead to an optimistic estimation of the risk in shutdown.

IAEA-TECDOC-1144 [1] suggests that a screening criterion of 10^{-12}/hour (equivalent to approximately 10^{-8}, if the POS duration were 1 year) could be adopted if the PSA model is intended for use in risk monitoring or maintenance scheduling.

5.3. External Hazards

The initiating event frequency for external hazards and also other events can vary during the year. The frequencies in the baseline PSA might represent the average yearly frequencies for such events. In the application PSA model, it is desirable that only events that pose a risk during the shutdown period should be considered which can be handled using environmental factors in the risk monitor.

For instance, extreme snow is only relevant to include during winter and the risk of organic material blocking the screen houses might only be a risk during summer.

6. CONCLUSION

Risk monitors can be a helpful tool to optimize outages and minimize risks. Experience from Ringhals shows that a straight-forward modification of the baseline PSA model into an application model reflecting point-in-time CDF for use in RiskWatcher can give important insights about plant vulnerability and risks of equipment unavailability due to outage activities in different plant operating states.

The PSA model modification, that included adjustments to remove asymmetrical assumptions in the PSA model, rescaling of frequencies from risk-per-year to risk-per-year-in-POS, and construction of an all-embracing analysis case to calculate core damage frequency in RiskWatcher was a time-consuming project. The decision to have the application PSA model integrated in the baseline PSA model makes it easier to maintain and keep updated but at the same time it makes the baseline PSA model more complex and difficult to navigate.

Risk-informed decision making is used more and more in the nuclear industry, but in order to draw the right conclusions based on PSA, for instance which plant operating state is favorable for a repair activity from a risk perspective, a higher resolution of the application PSA model might be required. In order to make results for different POSs comparable and reflect plant risk correctly, the resolution of the application PSA model might need to be higher than of the baseline PSA model, e.g.:

- Different treatment of time-based and demand-based frequencies for initiating events in the application PSA model.
- The screening of events in the baseline PSA model for shutdown might need to be revised for the application PSA model, not to exclude events with high instantaneous risk.
- Only events that pose a risk during the shutdown period should be considered – external hazards can vary during the year.

References

[1] International Atomic Energy Agency, "*Probabilistic safety assessments of nuclear power plants for low power and shutdown modes, IAEA-TECDOC-1144*", IAEA, 2000, Vienna