Shutdown PSA for Ringhals NPP Unit 1. Insights, overview and results.

Stefan Eriksson[a*], Marie Gryte[a], and Erik Cederhorn[b]
[a] Ringhals AB, Väröbacka, SWEDEN
[b] Risk Pilot, Stockholm, SWEDEN

Abstract: During 2011, 2012 and 2013 a Shutdown PSA (SPSA) has been developed for Ringhals NPP unit 1. Ringhals 1 is a Boling Water Reactor (BWR) made by ASEA-Atom situated at the West coast of Sweden. The SPSA supplement the existing PSA Level 1 and 2 for Ringhals 1 and the final outcome will give a complete risk profile for the unit, providing support for verification of plant safety and upgrades. This paper gives an overview of the level 1 SPSA. A description is made of the basic conditions for identification of Plant Operating States (POS), analysis of initiating events, sequence analysis and system analysis. The result for level 1 SPSA of R1 is briefly discussed.

Keywords: PSA, NPP, Shutdown conditions.

1. INTRODUCTION

Ringhals 1 is a Boiling Water Reactor (BWR) at a four-reactor site in the West coast of Sweden. During 2005 - 2009, Ringhals 1 has been undertaken a large modernization program including an additional I/C system, new diesel generators and a new cooling water supply chain. The program was initiated partly by findings in the previous Probabilistic Safety Assessment (PSA) analysis and partly by new regulations and demands from the regulatory body.

Several PSA studies have been made for Ringhals 1. The present study originates back to 2000 but has been complemented, revised and updated several times. The R1 PSA for at power is a full-scope PSA Level 1 & 2 covering both internal, external and area events. In the work with the upgrading of the reactor, the PSA model has been fully revised, e.g. the modeling of a Digital RPS complementing the old analogue RPS. For more information about findings and results see PSAM10-paper No. 14 - *Use of PSA in a Modernization Program. Findings and Results from the Ringhals 1 PSA*. Concerning details about the digital I&C refer to PSAM10-paper No. 110 - *Development of the Ringhals 1 PSA with regard to Implementation of a Digital Reactor Protection System*.

In 2011, Ringhals AB decided that an updated analysis of the remaining plant operating modes (POM) should be developed that would be integrated with the existing PSA. During 2011 to 2013 a PSA has been developed for shutdown operation. Today the shutdown study only includes PSA Level 1 and internal and external events. At the end of this year the SPSA will include a full-scope PSA Level 1 & 2 covering internal, external and area events.

* stefan.x.eriksson@vattenfall.com

2. OVERVIEW OF THE ANALYSIS

The analysis follow the main task in a SPSA Level 1 and 2, see figure 1. At Ringhals AB, the general procedure of performing a PSA is described in figure 1. The SPSA follow
that procedure in all aspects.

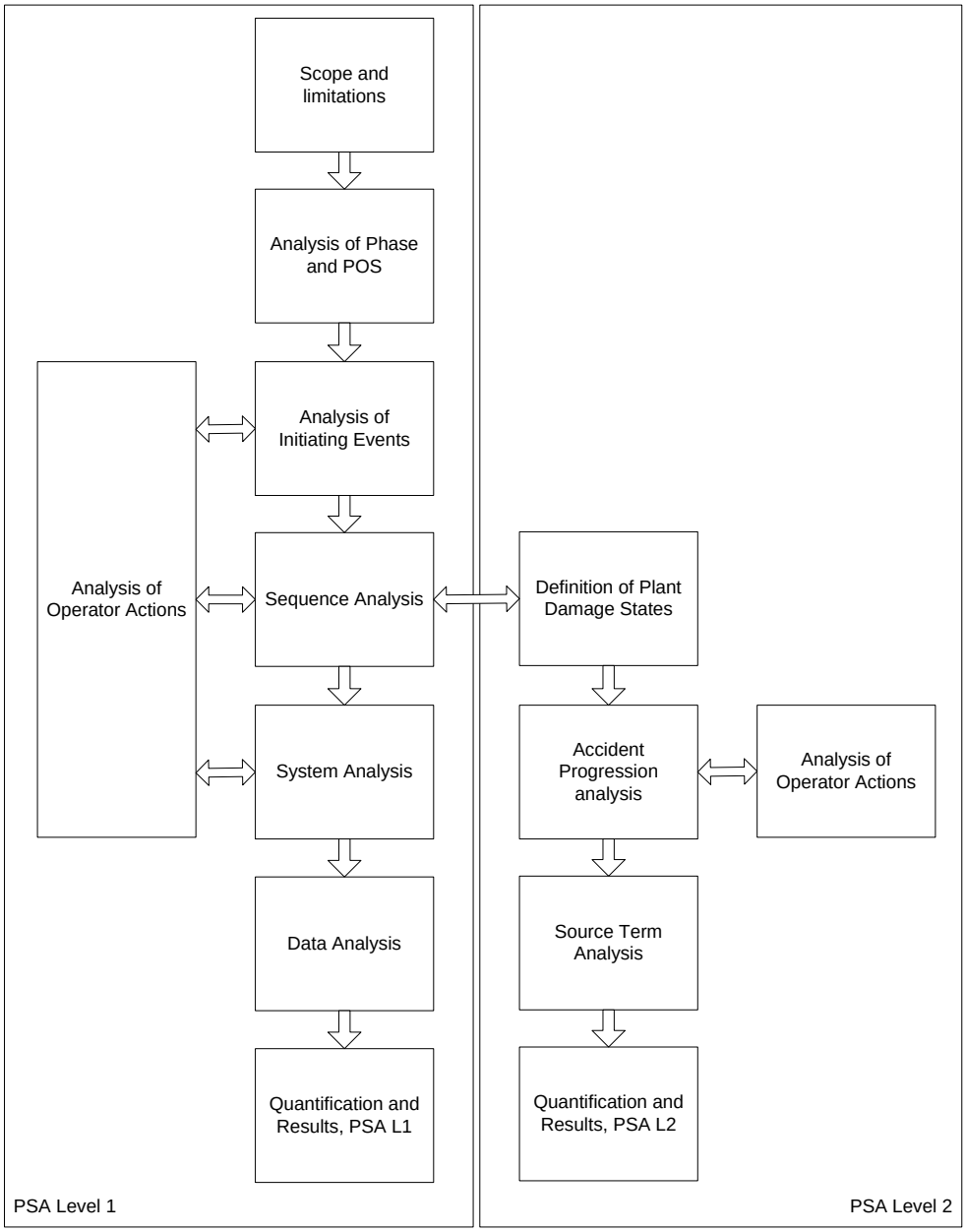

Figure 1 The main tasks in a SPSA Level 1 and 2

This paper describes main task for PSA Level 1. The procedure follows [1].

3. PLANT OPERATING STATES (POS)

Based on the shutdown procedure for Ringhals 1, Plant Operating States (POS) were defined as described in table 1.

Table 1: Ringhals 1, Plant Operating States (POS)

Phase	Description	Closed/ Open Primary System	Reactor Vessel Level/C-pool	Power supply unavailable because of maintenance	Configuration Residual Heat Removal system	Total time [h]
K1	Cold shutdown – Reactor Vessel Head mounted, water level under streamlines	Closed	Normal	-	The residual heat removal system (321) is cooling RPV with two trains.	20
K2	Cold shutdown – Reactor Vessel Head mounted, water level above streamlines	Closed	Top filled/ top filled above steam lines	-	The residual heat removal system (321) is cooling RPV with two trains.	36
K3	Cold shutdown – Open Reactor Vessel	Opened	Empty reactor hall pools	-	The residual heat removal system (321) is cooling RPV with two trains.	41
K4	Cold shutdown – Open Reactor Vessel. 40 h -7 days. B-side unavailable	Opened	Reactor hall pools are filled	Power supply B unavailable	One train of the residual heat removal system (321) is cooling RPV. Two trains of spent fuel pool cooling system (324) is cooling the reactor hall pools.	169
K5:1	Cold shutdown – Open Reactor Vessel. 7-14 days. B-side unavailable.	Opened	Reactor hall pools are filled	Power supply B. 50% of the time (in phase K5)	Two trains of spent fuel pool cooling system (324) is cooling the reactor hall pools. One train of the residual heat removal system (321) is cooling RPV is in standby, but maintenance on 321 possible.	253
K5:2	Cold shutdown – Open Reactor Vessel. 7-14 days. A-side unavailable.	Opened	Reactor hall pools are filled	Power supply A. 50% of the time (in phase K5)	Two trains of spent fuel pool cooling system (324) is cooling the reactor hall pools. One train of the residual heat removal system (321) is cooling RPV is in standby, but maintenance on 321 possible.	337

Phase	Description	Closed/ Open Primary System	Reactor Vessel Level/C-pool	Power supply unavailable because of maintenance	Configuration Residual Heat Removal system	Total time [h]
K6:1	Cold shutdown – Open Reactor Vessel. 14+ days. B-side unavailable.	Opened	Reactor hall pools are filled	Power supply B. 50% of the time (in phase K5)	Two trains of spent fuel pool cooling system (324) is cooling the reactor hall pools. One train of the residual heat removal system (321) is cooling RPV is in standby, but maintenance on one 321 and one 324 possible.	561
K6:2	Cold shutdown – Open Reactor Vessel. 14+ days. A-side unavailable.	Opened	Reactor hall pools are filled	Power supply A. 50% of the time (in phase K5)	Two trains of spent fuel pool cooling system (324) is cooling the reactor hall pools. One train of the residual heat removal system (321) is cooling RPV is in standby, but maintenance on one 321 and one 324 possible.	785
K7	Cold shutdown – Open Reactor Vessel. , 1 bar.	Opened	Empty reactor hall pools	-	The residual heat removal system (321) is cooling RPV with two trains.	920
K8	Cold shutdown – Reactor Tank idle on flange	Closed	Normal	-	The residual heat removal system (321) is cooling RPV with two trains.	1016

Cold shutdown is defined according to Technical Specification, as a subcritical reactor with water temperature below 100°C and the two operation mode switches turned to state "0".

4. INITIATING EVENTS

Identification of initiating events was made with the same condition as for the power operation PSA, i.e. the cladding temperature will reach above 1204°C due to loss of water inventory, loss of cooling, or reactivity transients (defined as BS1 for core damage in the RPV, BS2 for core damage in the spent fuel pit and BS 3 for core damage due to exposure of fuel rod during load/unloading because of outage LOCA. A time frame of 20 hours is defined. To handle or distinguish cored damage after 20 hours separate consequences are defined. Other consequences that are analyzed are:

- Exceeding of HTG (Highest accepted limit for the Pressure Vessel), primarily cold over pressurization.
- Exceeding of HTG for the temperature in the fuel pool (> 60°C)

Sequences where residual heat removal has been effective during this time frame, are considered to have a stable safe end state.

The sources of radioactivity considered in the analysis are:

- Reactor Pressure Vessel (RPV)
- The Spent Fuel Pit (SFP)
- Exposure of fuel rod during load/unloading because of outage LOCA

An initiating event in this analysis is an event with potential for leading to any of the unwanted end states and that may require functions for:

- cooling of the fuel in the reactor vessel/spent fuel pit
- maintaining applicable parameters as pressure, level and temperature in the reactor vessel and in the spent fuel pit within allowed limits
- reactivity control

An initiating event in the PSA model for cold shutdown is defined as an event that requires one or more manual alternatively automatically initiates actions to bring the plant to a safe end state. A screening value of 1·10-7 per year is used. This means that events with a frequency lower than the screening value are screened out from further consideration in the analysis.

The following initiating event categories are considered:

- Internal events (process related)
- Area events
- External events

Reference reports and background material forming the basis of identification and analyses of initiating events were:

- Ringhals Licensee Event Reports (LERs)
- R1 Safety Analysis Report (SAR)
- Nordic Owner Group report regarding safety during shutdown conditions [2]
- Previous PSA analyses at Ringhals
- Previous PSA analyses in Sweden (especially earlier shutdown studies at Forsmark NPP)
- Reference literature
- Specific work groups at the NPP (experts) identifying events to occur during shutdown

The Master Logical Diagram which describes the initiating event process is presented in figure 2. The categorization of initiating events follow [2]. Observe that CCI is added to list of initiating events.

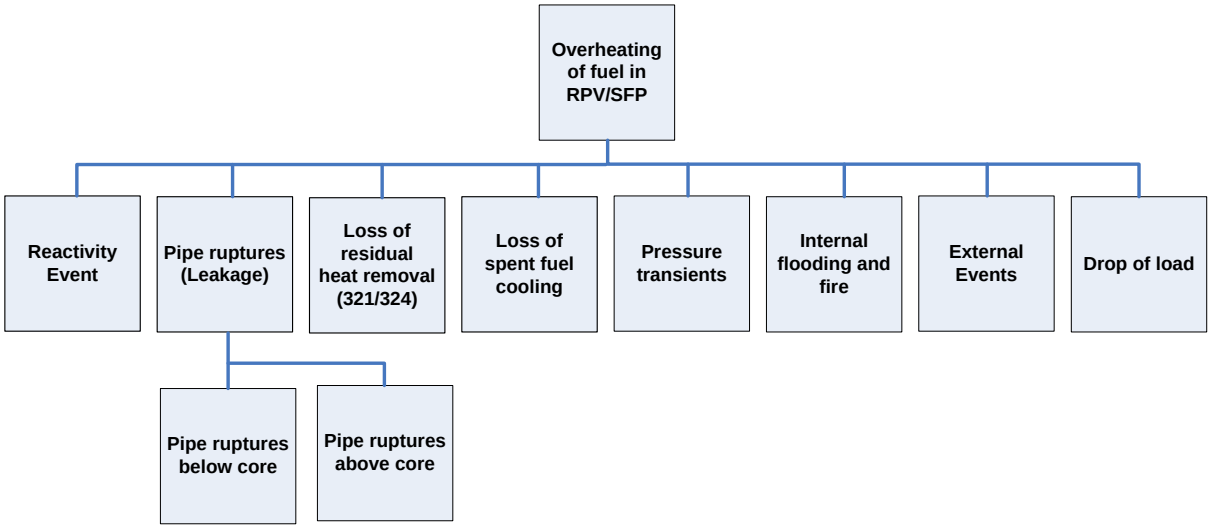

Figure 2: General Master Logic Diagram for overheating of fuel

5. SEQUENCE ANALYSIS

The sequence analysis follows the same model as for the power operation, thus it describes each sequence with a Success Block Diagram. All functions given in the Success Block Diagram (and subsequently in the event tree) are thoroughly described. The end state in the Success Block diagrams for the SPSA, Level 1 PSA will be some of the core damage consequences listed before (BSX) or safe state (OK). As far as possible, the structure of the full power PSA has been followed, but with focus on following functions:

- Pressure Relief and depressurization with system 314 and 326 (2 events for SPSA)
- Release of water to condensation pool through system 324 (1 event for SPSA)
- Water injection in Containment with system 733, 367 or 323 (3 events for SPSA)
- Closing of door between reactor pool and spent fuel pool (1 event for SPSA)
- Core cooling/Water injection in RC with system 416, 329, 733, 342, 322, 762, 323 (6 events for SPSA)
- Residual Heat Removal in RC/Containment with system 322, 321 or 324 (3 events for SPSA)
- Isolation functions leakage (3 events for SPSA)

For each of the identified initiating events, given in the previous chapter, a description is given as follows:

- Which POS are affected
- General success criteria
- Activation signals and time aspects

In all there are about 77 success block diagrams:

1. 14 for LOCA below the core
2. 18 for LOCA above the core
3. 4 for external LOCA below the core
4. 20 for external LOCA above the core
5. 4 for loss of residual heat removal due to loss of system 321 and/or 324
6. 4 for loss of residual heat removal due to CCI
7. 4 for loss of residual heat removal due to external events (loss of offsite power)
8. 4 for loss of residual heat removal due LOCA
9. 4 for loss of residual heat removal for spent fuel pool due to LOCA
10. 1 due to exposure of fuel rod during load/unloading because of outage LOCA

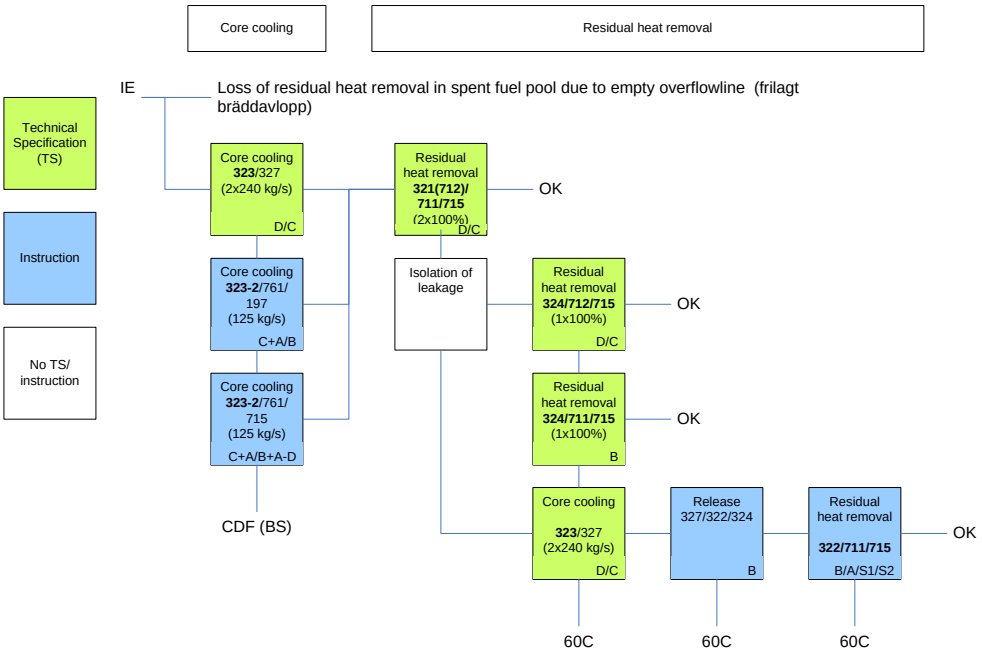

Figure 3: Success diagram for LOCA_221: LOCA 221 control rod drive mechanism (leakage below core, 76 mm)

6. SYSTEM ANALYSIS

The most important front line systems during shutdown conditions are

- System 314 – Pressure Relief System
- RH – System 321: Residual Heat Removal System
- SP – System 322: Containment Spray System
- SI – System 323: Safety Injection System
- System 326 – Reactor Vessel Head Spray System
- AF – System 329/416: Auxiliary Feedwater System
- SF – System 324: Spent Fuel Pool Cooling and Cleanup System
- System 367 – Mobile Pump for Containment Spray

In addition, the following support systems are covered by the systems analysis:

- CC – System 711: Cooling System for 321 and 322 (RHR and Containment Spray)
- SW – System 715: Salt Water System
- System 733 – Demineralised Water Storage and Distribution System
- FP – System 762: Fire Protection System
- Electrical system (overview)

For each system a description is given of:

- System Overview
- System tasks during shutdown
- System functions
- Assumptions and limitations
- Human actions related to system functions
- Fault tree modelling

7. HUMAN RELIABLITY ANALYSIS (HRA)

The included human interactions were divided according to IAEA-praxis [3], i.e. the categories A, B and C, where:

- Category A - Pre-incident tasks and errors
- Category B - Incident initiating errors
- Category C - Post-incident actions

Both screening analyses and detailed analyses were performed. The qualitative descriptions of the manual interactions, both for the screening- and detailed analyses, were emphasized.

7.1 Screening Analysis for Pre-Incident Tasks and Errors - Category A

The amount of category A actions are significantly lower in the outage analysis compared to the full power analysis. However, some category A actions are included in the outage analysis, and were identified departing from detailed descriptions of different scenarios. Screening values for category A actions were calculated based upon tables from e.g. THERP [4]. One example of an important category A action is the correct lining up of system 323 when performing maintenance on components which are critical from an outage-LOCA point of view.

7.2 Screening Analysis for Initiating Events – Category B

Manually initiated events for e.g. outage LOCA, loss of residual heat removal, and drops of heavy loads were analysed. For these three types of initiated events, different approaches were applied related to the explicit modelling. The most explicit modelling was done for the analysis of outage LOCA. For drops of heavy loads a semi-detailed analysis was done.

7.2.1 Screening Analysis for outage LOCA

In figure 4 the general model for analyzing outage LOCA is presented. For each of the sections in the figure a further subdivision is made. As an example, the section “possibilities for leakage when dismantling the component” consist of four different characterizations (D – Dismantling):

- D1 – A continuous and gradually increasing leakage will always occur in connection with the task, even if the task is not correctly performed. In order for a total (full scale) leakage to occur, the dismantling should be conducted for more than a minute despite of the increasing leakage.
- D2 – An abrupt leakage can occur even if the work procedures for dismantling the component are performed correctly.
- D3 – If the procedures for dismantling are followed on an overall level, but a couple of important steps in the procedure are not followed, there might be a leakage.
- D4 - If the dismantling is performed and a rather large deviation is done compared to what is stated in the procedures, there is a possibility that at leakage will occur.

For each characterization criteria (D1, D2, D3, D4, L1, L2 etc.) probabilities are assigned.

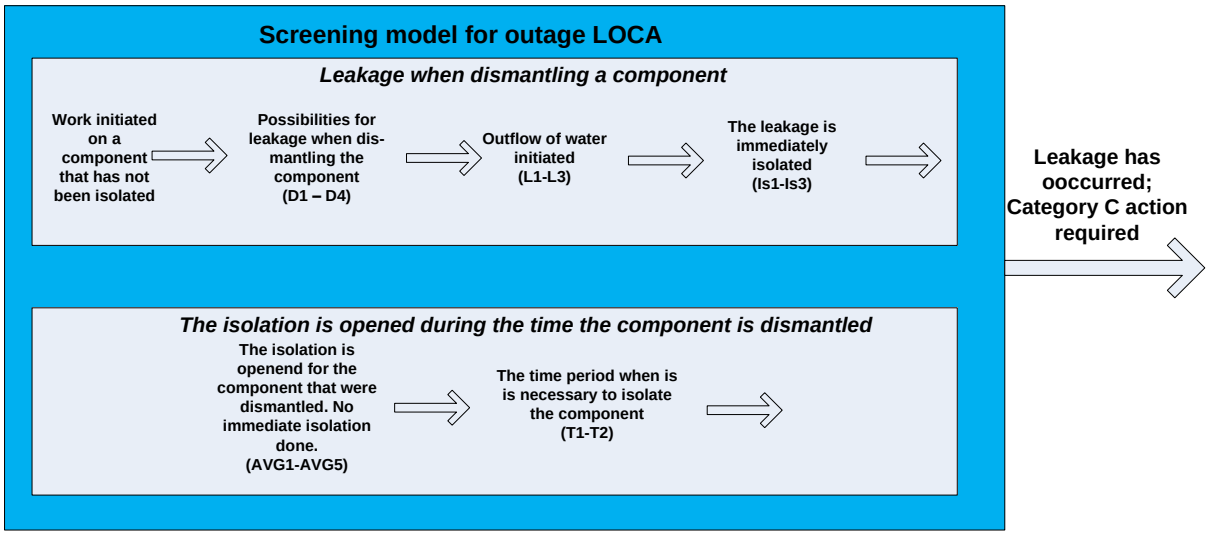

Figure 4: Screening model for outage LOCA

The general formula for estimating the probability for manually initiated outage LOCA for a specific component thus is:

$$P(\text{leakage}) = f(D/R, L, Is) + (AVG,T)$$

7.2.2 Screening Analysis for Loss of Residual Heat Removal

The probabilities for loss of residual heat removal due to manual interaction were estimated by using an expert judgment process (Delphi-influenced), in which three subject matter experts (SME) participated. They estimated the probabilities for losing systems that could either directly or indirectly lead to the initiating event, and both recoverable and unrecoverable loss of the systems were estimated. In table 2 two examples are shown.

Table 2: Example of probabilities for the loss of residual heat removal, on a systems level. For 90% of the cases the lost system can be repaired, for the other 10 % it is assumed that the lost system is unrecoverable.

System	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7	Phase 8
7xx	9,8E-4	7,9E-4	2,5E-4	6,3E-3	8,3E-3	2,2E-2	6,6E-3	4,8E-3
6xx	5,6E-4	4,5E-4	1,4E-4	3,6E-3	4,7E-3	1,3E-2	3,8E-3	2,7E-3

7.2.3 Detailed analysis for initiating events

For a number of manually induced initiating events that contributed significantly to the core damage frequency, detailed analysis were done. Based upon several interviews, procedures, drawings and in some cases inspection of the actual work environment hierarchical task analysis (HTA) were made. These HTAs were then complemented with tabular task analysis in which for example possible errors, error mechanisms, consequences and barriers were identified. Performing shaping factors relevant for the respective works were identified and estimated, i.e. on a five grade scale ranging from “very bad support” to “very strong support” for the work. Finally, error probabilities for possible human errors were quantified based upon a Delphi-influenced expert judgement process. Three different estimates were made, i.e. the median value for the human error, as well as the values for the 5th and the 95th percentile. A triangular shaped distribution was assumed.

7.3 Screening Analysis for Post-Incident Actions - Category C

For manual actions that aim to prevent the initiating events from leading to core damage, or exceeding of HTG, an approach departing from THERP's time-diagnosis curve were used [4, 5, 6]. Five calibration factors (performing shaping factors) were applied [5, 6]. Based upon the result for these calibration factors and the available time for resolving the problem (i.e. primarily based upon the time from the initiating event to core damage of exceeding HTG, subtracting times for e.g. implementing actions) a probability for failing with the manual action were calculated. The following calibration factors were used and their values were estimated by SMEs:

1. Quality and importance of procedures
2. Quality and importance of training
3. Feedback from process, quality of MMI
4. Mental load
5. Communication and coordination

In a few cases the time-reliability curve were not used. These cases consisted of mitigation actions (including observation, diagnosis and decision) that were only marginally cognitively demanding. In these cases THERP's ARM model [4] was used.

As a basis for all category C actions a rather detailed qualitative analysis were made, based upon interviews, procedures, HTAs etc.

7.4 Dependences

For assessing dependencies THERPS model [4] were applied.

7.5 Uncertainty Estimates and Reasonableness

Both uncertainty estimates and estimates of reasonableness were made for most of the included human interactions. The uncertainty estimates were done either by estimating the Beta-factors (primarily for the screening analysis), or by using Monte-Carlo simulations when performing Delphi-based expert judgments. When estimating the reasonableness of the results, the SMS reviewed the final results, primarily focusing on the internal ranking of e.g. the probabilities for manually initiated outage LOCAs for different components. Comparisons with actual data were done when such data existed. On a general level, the results were found to be reasonable.

In some cases the actual reasonableness for the actual human error probabilities were made. One example of the outcome from this was that the human error probability was not reasonable. In this case, the time reliability curve had been used when it was more justified to use the ARM-model.

8. RESULTS

The modelling of SPSA has been done in the same PSA model as for the R1 power operation model, i.e. the same Risk-Spectrum model has been used. The quantification has been done for internal events (including man-made initiating events) and the external event Loss of Offsite Power.

The preliminary results for level 1 SPSA of Ringhals 1 (to be finalized later this year) shows that the core damage frequency for the shutdown period is lower than for the full power operation mode but not significantly. The Plant Operating States 1 (cold shutdown. Reactor Vessel Head mounted, water level under steam lines) gives the largest contribution to the core damage frequency.

The preliminary results also show that there are no dominating sequences. The contribution from the sequence of highest order is just below 35 %. The relatively low core damage frequencies are probably due to:

- Events leading to cored damage after 20 hours not included in the results are sent to authorities
- Another reason for the low results is that events in the spent fuel pool are not considered in the results sent to the authorities
- Regulated and restricted instructions for which systems are to be operated during shutdown conditions

9. CONCLUSION

As for the preliminary results, the Level 1 SPSA indicates that the unit has large safety barriers during shutdown conditions. However, the final result must be studied before any final conclusion is made. From a PSA standpoint, the development of a Shutdown PSA does not differ much from an ordinary PSA. It is the author's belief that it is important to have an integrated model for all power operation modes. It is also important to have one common structure of the documentation. Having done that, it is fairly easy to progress with the PSA analysis. The difficulties lay, as always, in finding proper calculations (e.g. thermo hydraulics calculations of drain down events) in order to have the proper time frames. But that is probably the ever-remaining task for a PSA analyst, what is the available time for recovery actions?

An extensive amount of work is focused on a complete mapping of initiating events, even more compared to most other shutdown studies in Sweden. For example, every component (pumps and valves) in system connect to the reactor vessel and out to the isolation valve is mapped and analyzed regarding leakage rate, possibilities to isolate, level of studs and initiating frequency. Also the method for screening of possible initiating LOCA events inside containment due to faulty manual actions according is unique.

Because of the focus on a complete mapping of events showed that there were some events were core damage occurred after 20h (normal focus is on sequences with core damage occurred before 20h). To handle this type of event separate consequences was created. This feature makes it possible to analyze events with core damage after 20h.

Another unique feature compared to other shutdown studies is that the model also evaluate following events:

- Loss of residual heat removal for spent fuel pool due to outage LOCA
- Exposure of fuel rod during load/unloading because of outage LOCA

The biggest advantage of the new updated shutdown PSA for Ringhals NPP Unit 1 is that the model will support the possibility to analyze and plan future outages in a thoroughly and complete risk perspective.

Acknowledgements

The authors wish to acknowledge the support from Lennart Isaksson, Stefan Johansson and Stefan Peterson, operation support at Ringhals 1, for their support and wise words during the development and performance of SPSA.

References

[1] *A IAEA TECDOC-1144 - Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes,* March 2000

[2] *NOG - Säkerhet och Miljö. Säkerhet under revisionsavställning. Delprojekt B - Komplettering av befintlig säkerhetsredovisning*, 2003-11-21

[3] *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice.* IAEA Safety Series No. 50-P-10

[4] Swain, A.D., & H.E. Guttman, *"Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications"*, NUREG/CR-1278/SAND80-0200, Sandia National Laboratories for the U.S. Nuclear Regulatory Commission, Washington, DC, August 1983

[5] Holmberg, J.-E., Kent Bladh, K., Oxtrand, J., Pyy, P. *Enhanced Bayesian THERP — Lessons learnt from HRA benchmarking.* Proc. of PSAM 10 — International Probabilistic Safety Assessment & Management Conference, 7–11 June 2010, Seattle, Washington, USA, IAPSAM — International Association of Probabilistic Safety Assessment and Management, paper 52.

[6] Holmberg, J.E. & Pyy, P. *An Expert Judgement Based Method for Human Reliability Analysis of Forsmark 1 and 2 Probabilistic Safety Assessment.* PSAM 5, International Conference on Probabilistic Safety Assessment and Management, November 27 – December 1, 2000, Osaka, Japan.