An approach to analyse human reliability during refuelling outage of a nuclear power plant

Kent Bladh,[1] Jan-Erik Holmberg,[2] Ulf Kahlbom,[3] Jan Nirmark,[1] Erik Sparre[3]

[1] Vattenfall Power Consultant, Box 527, SE-162 16 Stockholm, SWEDEN
[2] VTT, P.O. Box 1000, FI-02044 VTT, FINLAND
[3] RiskPilot, Kungsholmsgatan 11, 3 tr, SE-112 27 Stockholm, SWEDEN

[2] *+358-20-722 6450, +358-20-722 6027, jan-erik.holmberg@vtt.fi*

Abstract

Human reliability analysis (HRA) constitutes a central role in the probabilistic safety assessment (PSA) for the low power and shutdown period of a nuclear power plant. This is because a large number of operative and maintenance activities take place during a refuelling outage when the plant, to a great extent, is disassembled, maintained, and then reassembled back to operational mode. The paper presents the HRA approach used in the shutdown PSA for Forsmark 1/2 and 3 nuclear power units in Sweden. Challenges of the analysis comprises handling the large scope of activities to be analysed, development and use of a quantification method consistent with the full power PSA, and integration of HRA with the "technical" part of PSA. Experiences from the analysis and results will also be discussed.

1. INTRODUCTION

A nuclear power plant (NPP) can be in many operational states, with reactor power ranging from full power to complete shutdown. Experience from shutdown PSAs (SPSA) shows that shutdown operating states can be significant contributors to a nuclear power plant's overall risk level. Important reason for this result is that, traditionally, less attention has been given to the design and operational features of nuclear power plants for these operational states. The variability in plant configurations, simultaneous unavailability of systems, reduced functionality of nuclear barriers and defence-in-depth, blocking of automatic actuation of safety systems and limitations in operational procedures are the main risk significant characteristics for low power and shutdown operational states. Although an SPSA is similar to a full power PSA in many respects, an SPSA may address important additional concerns relating to safety. These include simultaneous system unavailability during different phases of an outage, the importance of operator actions to restore functions, and the wide range of activities taking place during shutdown.

The key objectives to perform SPSA are:

- To increase awareness of the risks on a plant in the shutdown state
- To identify areas of safety improvement.

An SPSA can provide useful insights and feedback as regards: (a) outage planning; (b) plant operations and procedures during an outage; (c) shutdown technical specifications; (d) outage management practices; (e) personnel training; (f) emergency planning and emergency operating procedures and (g) hardware modifications. Regarding such applications, risk from all operating states should be considered in an integrated manner. Hence, the SPSA should be considered in the context of the full scope PSA. For example, moving maintenance activities from shutdown operating states to full power operations and changing the duration of allowed

outage times in technical specifications could affect not only the shutdown PSA, but also the full power PSA. An isolated view based only on changes in shutdown risk for individual applications, without consideration of the risk impacts during other operational states, might be misleading.

2. SHUTDOWN PSA FOR FORSMARK 1/2 AND 3 NPP UNITS

Forsmark 1/2 and 3 NPP units are boiling water reactors (BWR) located in Sweden 170 km north of Stockholm. Forsmark 1/2 are identical units being in commercial operation since 1980 resp. 1981. Forsmark 3 has slightly newer design and has been in commercial operation since 1985. From PSA point of view, there are lots of similarities between the units but there are differences in design and operational features for which reason Forsmark 1/2 has a common PSA and Forsmark 3 unit has a PSA of its own.

The latest updates of PSAs (2005–2006) for Forsmark 1/2 and 3 NPP units include a comprehensive analysis of core damage risk during low power and shutdown operating states. Practically, the update project was divided into a technical PSA part and HRA part [1].

In the analysis, the shutdown period is divided into the plant operating states (POS) shown in Table 1 and Figure 1. For each POS, potential initiating events and required safety functions were identified, success criteria of safety functions were defined and configurations of safety systems were analysed. Based on this analysis several event trees were created for each POS and the system fault trees developed for full power PSA were modified to match with POS-specific conditions. As can be seen, a shutdown PSA model is in fact a set of POS-specific PSA models, and is thus much more extensive than a full-power model. Full power PSA can be used as a basis for many parts, but, e.g., analysis of initiating events and sequence analyses are unique to SPSA. HRA is a significant part of these analyses unique to SPSA.

Table 1. Plant operating states (POS) in shutdown PSA for Forsmark 1/2 and 3.

POS	Description
K1	Cold non-pressurised reactor (p = 1 bar, T<100 °C), reactor pressure vessel lid mounted, normal water level in reactor pressure vessel
K2	Cold non-pressurised reactor, reactor pressure vessel lid mounted, water filling of reactor pressure vessel from normal level to flange level
K3	Reactor pressure vessel lid dismounted (open primary circuit), reactor pool empty
K4.1	Open primary circuit, reactor pool full
K4.2	Refuelling, residual heat removal with systems 321 (shutdown reactor cooling system) and 324 (pool cooling system)
K4.3	Refuelling, residual heat removal with systems 324
K4.4	Open primary circuit, reactor pool full
K5	Open primary circuit, reactor pool empty
K6	Reactor pressure vessel lid mounted

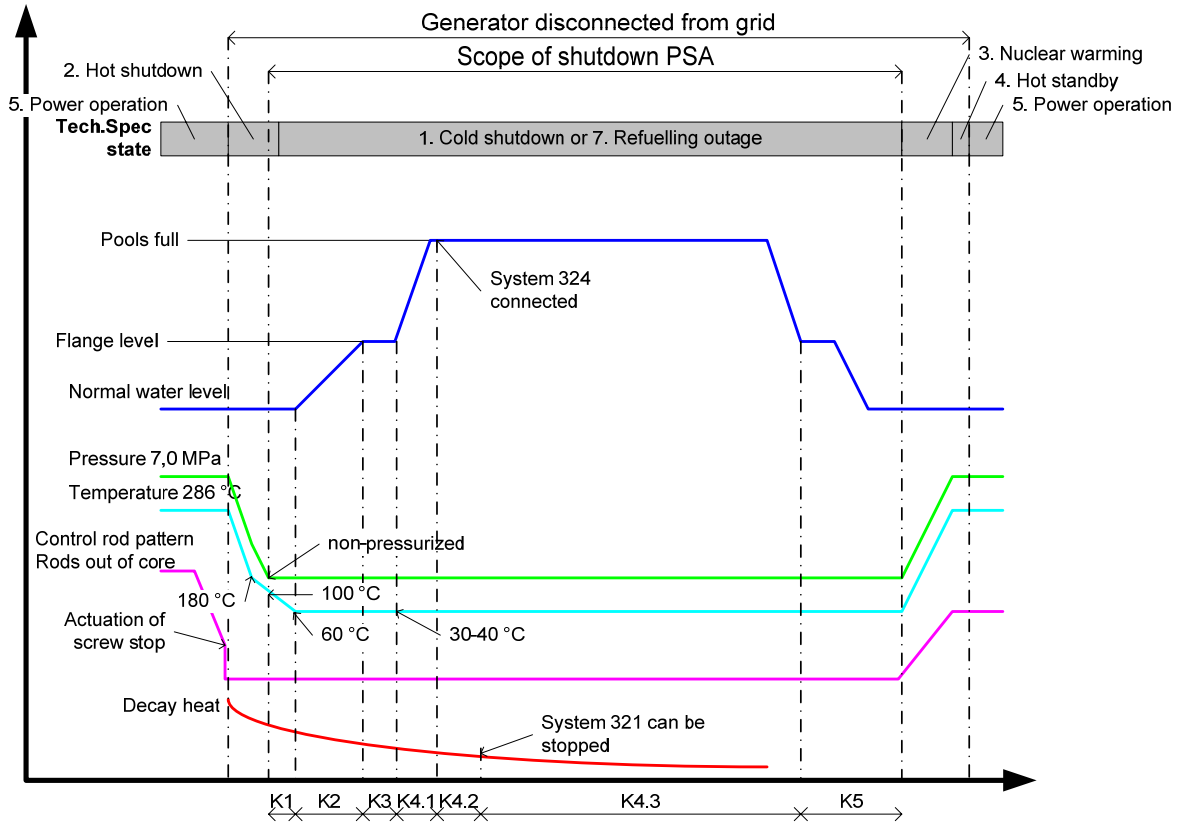

Figure 1. Plant operating states (K1, K2, …, K5) in shutdown PSA and main process parameters for Forsmark 1/2 and 3. Systems 321 and 324 are important for residual heat removal.

3. APPROACH TO HUMAN RELIABILITY ANALYSIS

The approach used for analysis of human reliability in Forsmark 1/2 and 3 SPSA was to many extent conventional, e.g. following the division of human interactions into three categories:

- Pre-initiator actions (Type A)
- Initiating actions (Type B)
- Post-initiator actions (Type C).

The analysis of pre-initiator actions (type A) includes human interactions that can cause unavailabilities in safety-related systems. These include both intentional unavailabilities due to maintenance, repair and testing actions and unintentional unavailabilities due to deficient or missing restoration of equipment, after intentional actions. The number of intentional unavailabilities is large during a refuelling outage, and it is a complex task to estimate these unavailabilities in each POS. A conservative approach is to assume that the minimal amount of the trains of the safety systems, allowed by the safety technical specifications of the plant, is operable. If this assumption leads to high risk numbers, the truly experienced unavailabilities need to be explored from operating and maintenance records. Regarding unavailabilities due to deficient or missing restoration of equipment, the full-power PSA analysis can be used as a starting point. This can be a conservative assumption, since compared to full-power scenarios, there is usually more time to restore the equipment in SPSA scenarios.

The analysis of human caused initiating events (Type B) is one of major tasks in an SPSA. In the Forsmark case, the analysis was based on a list of initiating events compiled by Nordic

Owner's Group for boiling water reactors. Despite of a comprehensive list of scenarios to be analysed, a lot of work is still needed to verify the relevance of each scenario to a specific nuclear power plant unit. This analysis was carried out by interviewing operating and maintenance staff and by walk-throughs of working procedures. The human errors were quantified using the procedure shown in Figure 2. The same method was used for human errors leading to deficient restoration of equipment (Type A human error).

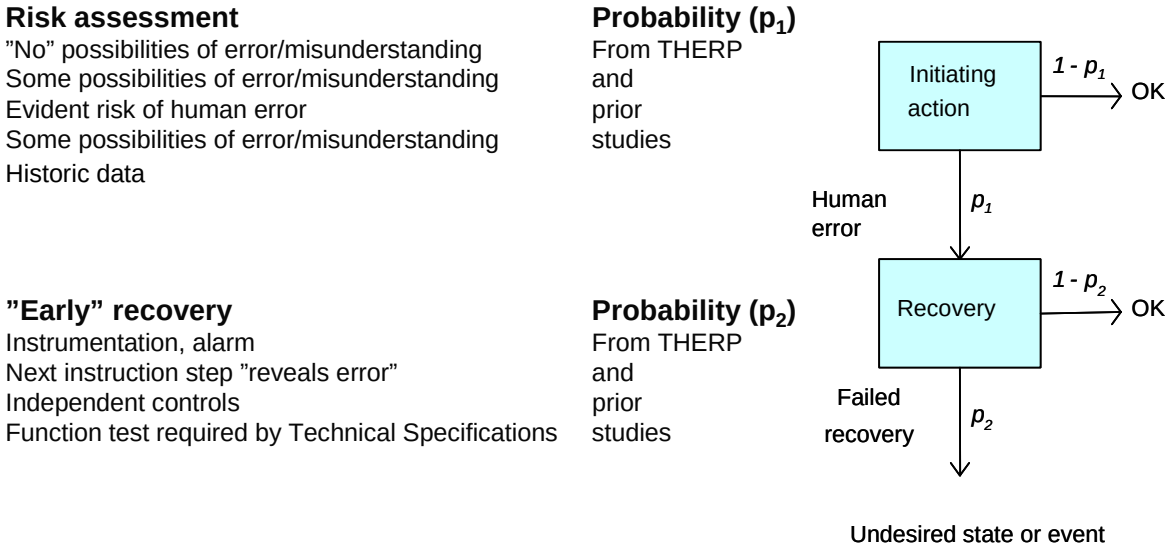

Figure 2. Quantification scheme for human error leading to deficient restoration of equipment (Type A human error) or to an initiating event (Type B human error). THERP = Technique for Human Error Rate Prediction [2].

The analysis of post-initiator human interactions is principally similar to the one used in full-power PSA. Particular challenges in the SPSA context are:

- Operator actions are important for successful management of disturbances. In full-power scenarios, operator actions are back-up functions.
- Several parties can be involved in actions because local manoeuvres are needed, i.e., main control room crew, maintenance personnel, fire and rescue brigades.
- Several actions can be needed to control the situation.
- Instructions may provide little support.
- Uncertainties in the course of events (specifically in loss-of-coolant-accident, LOCA, scenarios) regarding which actions are necessary to balance the situation and whether some actions can have negative influence on safety functions.

Operator actions were identified and defined in an iterative manner together with (technical) PSA-team and control room operators. Since instructions do not provide support to all scenarios, it is not obvious which actions should be accounted in the analysis.

Another aspect to be addressed in the definition of operator actions is the dependencies between the actions. Therefore attention was paid to control the number of operator actions that should be modelled as basic events in PSA. Preferably the basic event should cover as large entity (= whole safety function) as possible. Fault tree analysis was used in this analysis process (see Figure 3).

The same quantification method was used as in the power-operation analysis, i.e., time-dependent human error probability taken from Swain's handbook [2] adjusted with calibration factors reflecting the following performance shaping factors: (1) support from procedures, (2) support from training, (3) feedback from process, (4) need for co-ordination and communication, (5) mental load, decision burden [3, 4].

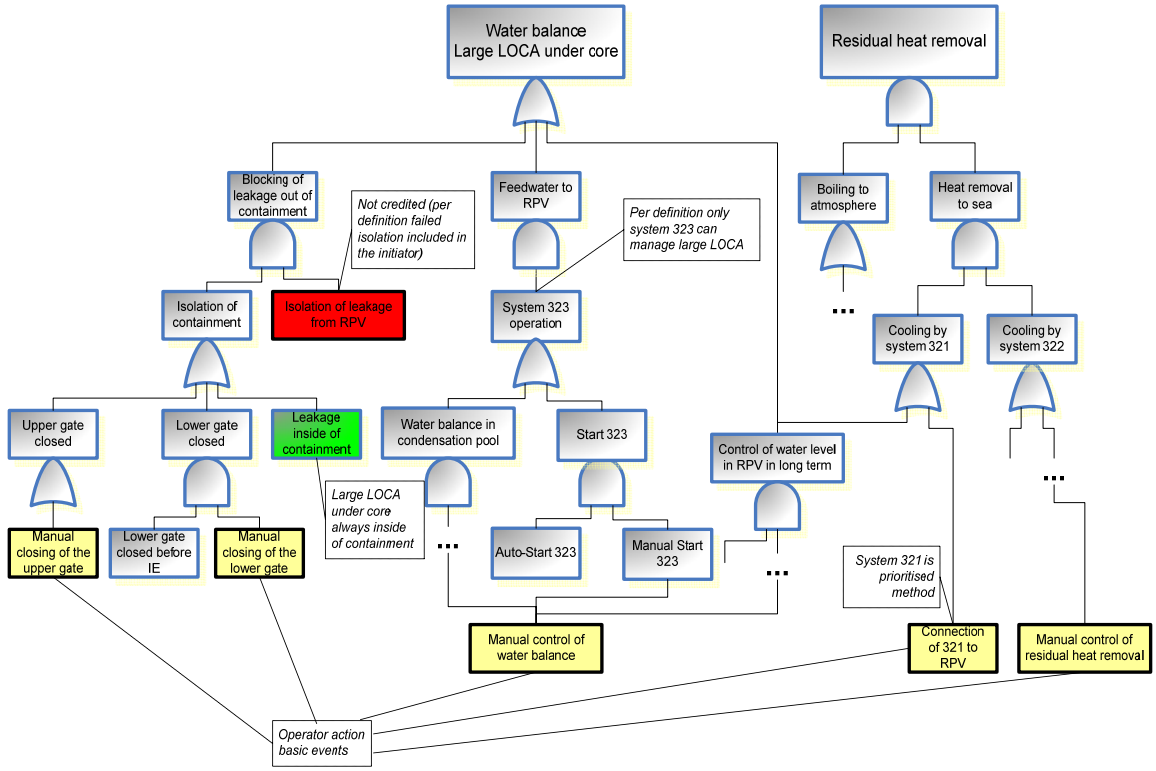

Figure 3. Fault tree method used in the definition of operator actions for the PSA model. Top boxes are the main safety objectives, yellow boxes the operator actions, red boxes conditions that are false (success logic) and green boxes conditions that are true (success logic).

4. CONCLUSIONS

Human reliability analysis (HRA) constitutes a central role in the probabilistic safety assessment (PSA) for the low power and shutdown period of a nuclear power plant. This is because of a large number of operative and maintenance activities take place during a refuelling outage when the plant, to a great extent, is disassembled, maintained and then reassembled back to operational mode. Challenges of the analysis comprises handling the large scope of activities to be analysed (so that all actions potentially contributing risk will be covered), development and use of a quantification method consistent with full power PSA, and integration of HRA with the "technical" part of PSA. HRA is an essential part of shutdown PSA.

5. REFERENCES

[1] K. Bladh, J.-E. Holmberg, J. Nirmark and J. Sandstedt, S*hutdown PSA for Forsmark 1/2 and 3.* Presented in the Nordic PSA Castle Meeting 2006, Varberg, Sweden September 26–27, 2006.

[2] A.D. Swain, and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. NUREG/CR-1278, Sandia National Laboratories, Albuquerque, USA, 1983, 554 p.

[3] P. Pyy, P., R. Himanen, A Praxis Oriented Approach for Plant Specific Human Reliability Analysis - Finnish Experience from Olkiluoto NPP. In: Cacciabue, P.C., and Papazoglou, I.A. (eds.), *Proc. of the Probabilistic Safety Assessment and Management '96 ESREL'96 — PSAMIII Conference*, Crete, June 24–26, 1996. Springer Verlag, London, 1996, pp. 882–887.

[4] J. Holmberg, J., and P. Pyy, An expert judgement based method for human reliability analysis of Forsmark 1 and 2 probabilistic safety assessment. In: Kondo, S. & Furuta, K. (eds.), *Proc. of the 5th International Conference on Probabilistic Safety Assessment and Management (PSAM 5)*, Osaka, JP, 27 Nov. – 1 Dec. 2000. Vol. 2/4. Universal Academy Press, Tokyo, 2000, pp. 797–802.