Development of Specific PSA-tailored ESDs: A real-case industrial-scale implementation

Rainer Hausherr[a] and Dusko Kancev[a],

[a] *Nuclear Safety, NPP Goesgen-Daeniken AG, Switzerland*

Organiser use only: Received date; revised date; accepted date

Keywords: PSA, event sequence diagrams (ESD), OA, EOP, EOC, HRA dependencies

Abstract: A major task in the development of a new industrial scale full scope PSA is the definition of the event trees for the level-1-PSA. For the large-scale project – PSASPECTRUM – migrating KKG`s existing PSA model from Riskman® to RiskSpectrum® environment, it was decided to use and develop detailed plant tailored event sequence diagrams (ESD) as basis for this task.
This paper addresses the development of detailed plant-tailored and PSA-related ESDs. These ESD show the behaviour of the plant given specific initiating events, for example a steam generator tube rupture. The behaviour of the plant is driven by the actuation signals of the reactor protection system (RPS), the designed functions of the frontline systems, the operator actions guided by the emergency operating procedures (EOPs) and the preventive actions defined in the severe accident management guidelines (SAMG). The ESD are developed in such a way that they include all the PSA-relevant operator actions together with the links to the dedicated tasks defined in the EOP and SAMG, and the impacts of failures of frontline systems. By focussing on RPS signals, operator actions, and failures of frontline systems, the ESDs achieve the goal to show the plant behaviour in a transparent way and to define the boundary conditions for the reliability analysis of the operator actions (HRA). To improve the transparency and clarity of the developed ESDs, modules are developed for some major functions. These modules are, in essence, identical parts of the ESD-logic, being repeatedly challenged in various ESDs for different initiation events, e.g. SG feedwater supply. In this way, each ESD defines the possible outcomes of an initiating event on about 4 to 6 pages.
The development of the ESD also serves the identification of errors of commission (EOC), as it is required in the guideline of the Swiss nuclear regulator. When developing the ESD, some weaknesses of the EOPs and SAMGs could be identified and amended. Potential improvement of frontline systems of the plant were also identified and are currently assessed, both probabilistically as well as deterministically.
By defining the relevant operator actions of a sequence, the ESDs also clearly outline potential HRA dependencies between/among operator actions and support the quantification of their dependencies. Such an assessment of dependencies between/among operator actions is also required by the Swiss nuclear regulator.
The paper concludes with an example assessing the effect of a potential plant improvement on different sequences during a steam generator tube rupture event.

1. Introduction

In July 2020, NPP Gösgen-Däniken AG (KKG) started the project (*PSASPECTRUM*) to redevelop its plant specific PSA model. The new model uses the *RiskSpectrum®* software suite, whereas the existing (old) PSA model uses RISKMAN®.
With the *PSASPECTRUM* project, KKG will achieve a consistent and comprehensive PSA model and documentation. With the new model all the relevant PSA applications shall be performed, and the national regulatory requirements shall be fulfilled more effectively.
The PSA-model will include all plant operating states (POSs) (full-power, low power & shutdown), all IEs classes (internal & external), all hazards (internal & external) and will fully couple level-1 and level-2.

One of the highlights of the project is the development of the new event sequence diagrams (ESDs). Two types of ESD have been developed: Module-ESD and initiating event ESD (IE-ESD). Module-ESD represent safety functions consisting of different system functions. The idea is that these modules can then be used in the ESD for initiating event to simplify their structure. IE-ESD show the behaviour of the plant and operators in response to an initiating event.

2. Development of the ESD

At KKG, flow charts are available giving a broad overview about systems needed for different types of initiating events. In addition, for the training of reactor operators, several sequence diagrams focusing on the expected plant behaviour for design base accidents were developed in the past. The expected plant behaviour follows the design concept of the plant, which is, for most safety systems, 4 x 100%. These sequence diagrams include a lot of operator actions serving a careful treatment and smooth cooldown of the plant. However, for the PSA operator actions required for preventing core damage and reducing radioactive releases are relevant.

Figure 1 below shows the module for feeding water to the steam generators. MFW: main feed water, AFW: auxiliary feed water, EFW: emergency feed water, SEFW: special emergency feed water. Operator actions instructed by EOP are marked blue, accident management actions guided by SAMG are marked reddish. The ESD distinguishes signals from RPS (marked with LT in the upper left corner of the blocks) and the hardware affected by these signals. Hardware functions are marked with VT in the upper left corner of the blocks. Every block is numbered for easy identification. Circles along paths of the ESD are used to summarize information about the sequence.

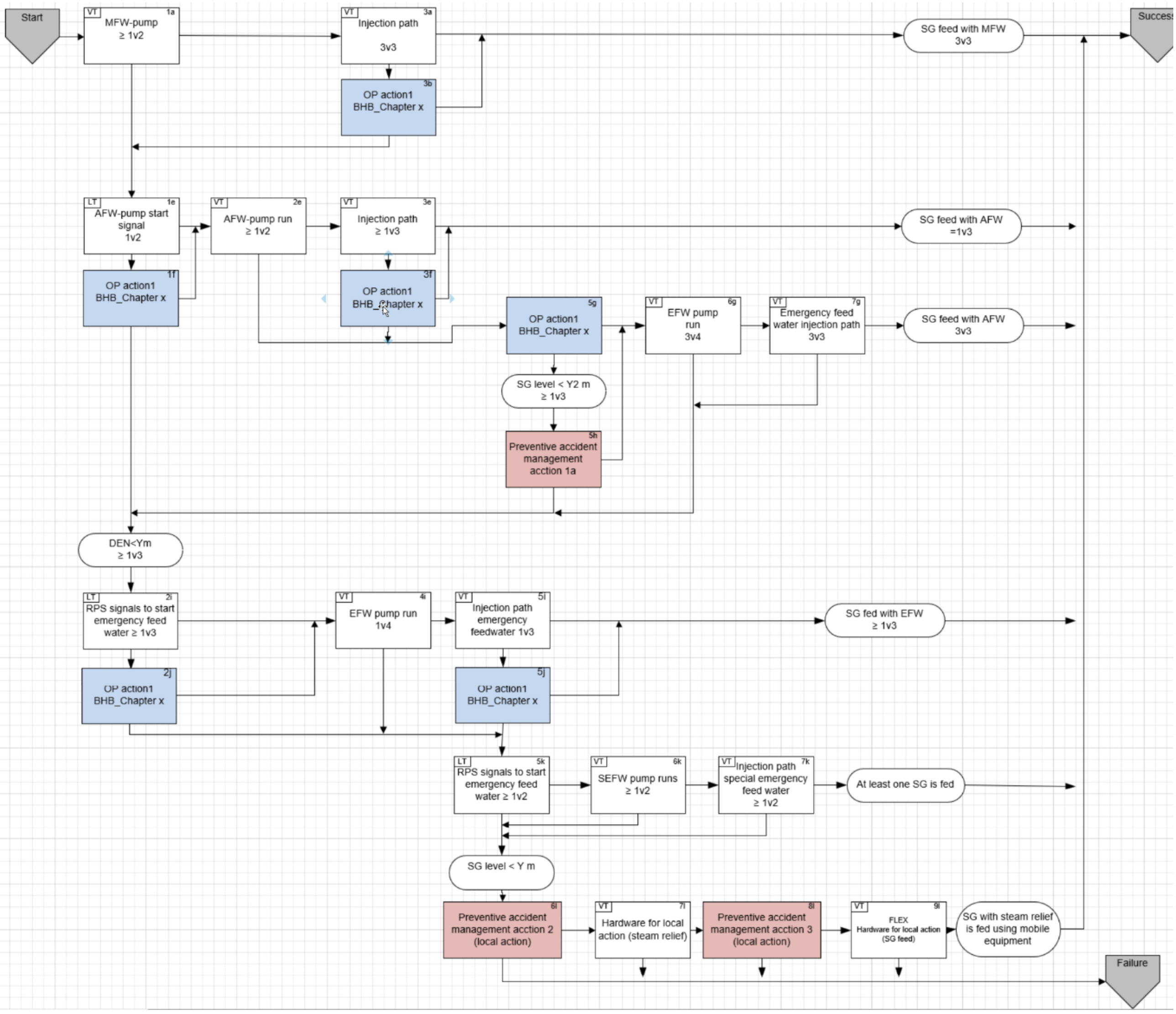

Start
VT 1a MFW-pump ≥ 1v2
VT 3a Injection path 3v3
3b OP action1 BHB_Chapter x
SG feed with MFW 3v3
Succes
LT 1e AFW-pump start signal 1v2
VT 2e AFW-pump run ≥ 1v2
VT 3e Injection path ≥ 1v3
SG feed with AFW =1v3
1f OP action1 BHB_Chapter x
3f OP action1 BHB_Chapter x
5g OP action1 BHB_Chapter x
VT 6g EFW pump run 3v4
VT 7g Emergency feed water injection path 3v3
SG feed with AFW 3v3
SG level < Y2 m ≥ 1v3
5h Preventive accident management acction 1a
DEN<Ym ≥ 1v3
LT 2i RPS signals to start emergency feed water ≥ 1v3
VT 4i EFW pump run 1v4
VT 5i Injection path emergency feedwater 1v3
SG fed with EFW ≥ 1v3
2j OP action1 BHB_Chapter x
5j OP action1 BHB_Chapter x
LT 5k RPS signals to start emergency feed water ≥ 1v2
VT 6k SEFW pump runs ≥ 1v2
VT 7k Injection path special emergency feed water ≥ 1v2
At least one SG is fed
SG level < Y m
6l Preventive accident management acction 2 (local action)
VT 7l Hardware for local action (steam relief)
8l Preventive accident management acction 3 (local action)
VT 9l FLEX Hardware for local action (SG feed)
SG with steam relief is fed using mobile equipment
Failure

Figure 1. ESD module for SG feedwater function

Such modules have been developed for several functions regarding secondary steam relief (relief using the safety valves, depressurisation using the steam generator relief valves), and isolation of the reactor coolant inventory following LOCA conditions.

The IE-ESD show the behaviour of the plant and the operators in response to an initiating event. They include all relevant hardware functions of front-line systems like feeding water into steam generators, depressurise the plant using the steam generators, high- and low-pressure injection into the RCS (reactor coolant system), sump recirculation and alignment of residual heat removal, isolation of systems etc. The IE-ESD also include the relevant signals from the RPS, the actions of the operators guided by the EOPs and the preventive part of the SAMGs. The IE-ESD address the individual steps in the EOC to directly support the assessment of the reliability of the operator actions (HEP). This required scrutinizing the EOPs for actions directly needed to prevent core damage. As EOPs are focusing on design base accidents, they include a lot of actions which are not required to prevent core damage. It required an intensive collaboration with the operational department until the crucial operator actions could be identified. In the end, the developed ESD are specifically PSA-tailored, because they contain all the information required for developing the event trees and quantifying operator actions and their dependencies.

The IE-ESD form the basis for developing the event trees in RiskSpectrum® PSA software.

Figure 2 below shows a part of the IE-ESD for steam generator tube ruptures (SGTR). When a tube in steam generator ruptures, inventory from the RCS transfers to the secondary side of the SG and can be released by the SG safety valves or relief valves. In this way, a direct path from the RCS to the environment is open. The part of the IE-ESD shown in Figure 2 presents the situation after successful SCRAM, turbine trip, available secondary feed water system and steam relief, and high-pressure safety injection (HPSI). This situation is characterized by the gray transfer gate on the upper left corner of Figure 2.
High pressure spray system must be aligned to reduce pressure in the RCS and in this way reduce the flow from the RCS into the SG with the broken tube and increase the level in the pressurizer (block 40a – 40c). If the spray system is not working (block 41a), venting the pressurizer is an alternative option (blocks 41b and 42b). When the level of the pressurizer is sufficiently high, HPSI pumps can be stopped. Stopping the HPSI pumps is done to prevent the level and pressure in the steam generators to high and therefore opening the safety valve and releasing steam and coolant inventory into the environment. As can be seen, stopping HPSI is addressed in two steps in the EOP (blocks 43a and 43b) and in one step in the SAMG (block 43c). After stopping HPSI the SG with the broken tube can be isolated. There are multiple steps in the EOP and SAMG guiding to this action (blocks 44a – 44d). With the SGTR isolated (block 45a) secondary heat removal using intact SG must continue (block 46a) to reach a stable condition.

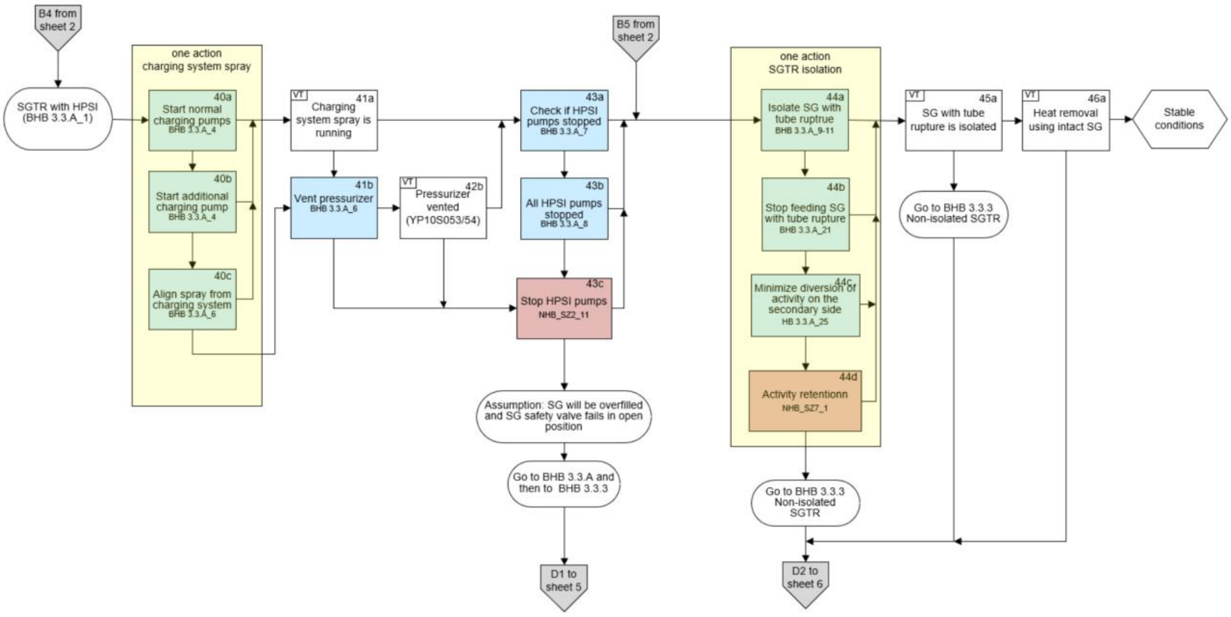

B4 from sheet 2
SGTR with HPSI (BHB 3.3.A_1)
one action charging system spray
40a Start normal charging pumps BHB 3.3.A_4
40b Start additional charging pump BHB 3.3.A_4
40c Align spray from charging system BHB 3.3.A_6
VT 41a Charging system spray is running
41b Vent pressurizer BHB 3.3.A_6
VT 42b Pressurizer vented (YP10S053/54)
43a Check if HPSI pumps stopped BHB 3.3.A_7
43b All HPSI pumps stopped BHB 3.3.A_8
43c Stop HPSI pumps NHB_SZ2_11
Assumption: SG will be overfilled and SG safety valve fails in open position
Go to BHB 3.3.A and then to BHB 3.3.3
D1 to sheet 5
B5 from sheet 2
one action SGTR isolation
44a Isolate SG with tube ruptrue BHB 3.3.A_9-11
44b Stop feeding SG with tube rupture BHB 3.3.A_21
44c Minimize diversion of activity on the secondary side HB 3.3.A_25
44d Activity retentionn NHB_SZ7_1
Go to BHB 3.3.3 Non-isolated SGTR
D2 to sheet 6
VT 45a SG with tube rupture is isolated
Go to BHB 3.3.3 Non-isolated SGTR
VT 46a Heat removal using intact SG
Stable conditions

Figure 2. Part of the ESD for SGTR

The gray transfer gates show either paths coming from or leading to other parts of the IE-ESD.

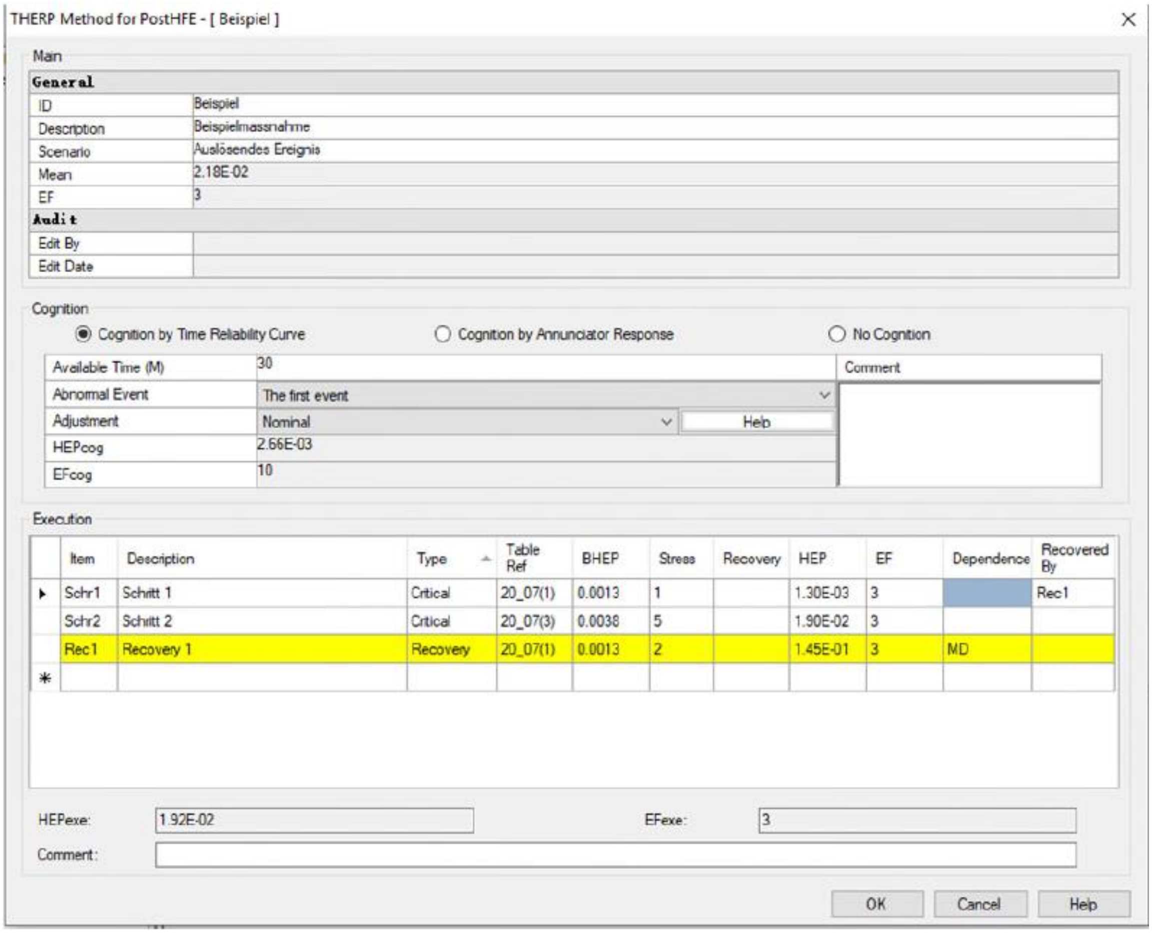
3. Modelling of Operator Actions

The operator actions (OAs) depicted on the various ESD are so-called Type C OAs. A Type C OA occurs after an initiating event. The operators must carry out defined tasks for the manual initialization, control and use of the systems and components for accident management and mitigation. These tasks are controlled by the accident procedures (e.g. EOPs or SAMGs, as explained above in text) and instructed in individual steps (step sequences). The ESD show whether an action is advised in one step of the EOC only or whether the action is advised with multiple steps in the EOC and/or SAMG. The HEPs for both the EOP and SAMG are quantified, in general, by using the THERP methodology [1].

The analyses of the manual measures are carried out in the program RiskSpectrum® HRA (RSHRA) [2] Version 1.0.0.4. The program can use different quantification methods for the same measure. Figure 3 shows an example of the analysis according to THERP.
In the "Cognition" part, the diagnosis is carried out according to THERP. A distinction is made between the 1st event and further events after the occurrence of the incident. The time reliability correlation (TRC) from the THERP methodology is used to evaluate the diagnosis, i.e. the probability of a diagnostic error depends on the available diagnostic time.

Figure 3. Example of an analysis with RiskSpectrum® HRA

Within the "Execution" part, each critical step is evaluated. Rows marked in yellow contain recovery measures that represent redundancy to one or more failed critical steps. Figure 3 shows the evaluation of an example measure in which step 1 ("Schritt 1") was carried out with a recovery measure. The rationale behind the applicability of recovery steps lies with the available personnel and/or available time for a certain accident scenario. Namely, in accident scenarios where e.g. the second shift manager is also available alongside the first one or maybe even the Pickett engineer is available in case of SAMG. There are also situations, when a blue block (EOP OA) within a certain ESD is followed on its failure path by a reddish block (SAMG OA) and both of their positive outcomes converge to the same point in the ESD. In this case, the existence of the SAMG OA as a redundancy to the EOP OA is in some cases not considered as a separate function event / Basic event in the ET-structure but rather being modelled as a recovery measure within the RSHRA modelling of the blue block.



THERP Method for PostHFE - [Beispiel]

Main

General	
ID	Beispiel
Description	Beispielmassnahme
Scenario	Auslösendes Ereignis
Mean	2.18E-02
EF	3
Audit	
Edit By	
Edit Date	

Cognition

● Cognition by Time Reliability Curve ○ Cognition by Annunciator Response ○ No Cognition

Available Time (M)	30	Comment
Abnormal Event	The first event	
Adjustment	Nominal	
HEPcog	2.66E-03	
EFcog	10	

Execution

	Item	Description	Type	Table Ref	BHEP	Stress	Recovery	HEP	EF	Dependence	Recovered By
▸	Schr1	Schritt 1	Critical	20_07(1)	0.0013	1		1.30E-03	3		Rec1
	Schr2	Schritt 2	Critical	20_07(3)	0.0038	5		1.90E-02	3		
	Rec1	Recovery 1	Recovery	20_07(1)	0.0013	2		1.45E-01	3	MD	
*											

HEPexe: 1.92E-02 EFexe: 3

Comment:

The nominal, white rows in the "Execution part" are modelling various errors of omission (EOO) as well as errors of commission (EOC) as constituent steps that are intended to be performed as part of a given accident procedure (EOP or SAMG).

In the control room, the shift manager instructs the measures to be carried out according to the short version of the BHB. If the measure is highlighted in white in the short version of the EOPs, the reactor operator can use the long version, but is not obliged to do so. If, however, the measure is highlighted in black in the short version, the shift manager instructs the reactor operator to use the long version. As mentioned above, the deputy, i.e. the second shift manager will be considered as recovery for errors of omission and/or commission with a medium dependency.

When determining the stress level, a distinction is made between the stress level for OAs in the main control room and the stress level for OAs on site. For the stress level in the control room, a distinction is made between OAs from the EOPs and measures from the SAMGs. Measures from the EOPs are generally more practiced and usually indicate that the accident can still be well controlled, while measures from the SAMGs are often more complex and their use indicates that the accident is more complex and more difficult to resolve. For these reasons, the stress level is determined as follows:

- For EOP OAs in the early phase (approximately first hour), increased stress (SF = 2) is assumed, then nominal stress (SF = 1).
- For SAMG OAs in the early phase, extreme stress (SF = 5) is assumed, then increased stress (SF = 2).

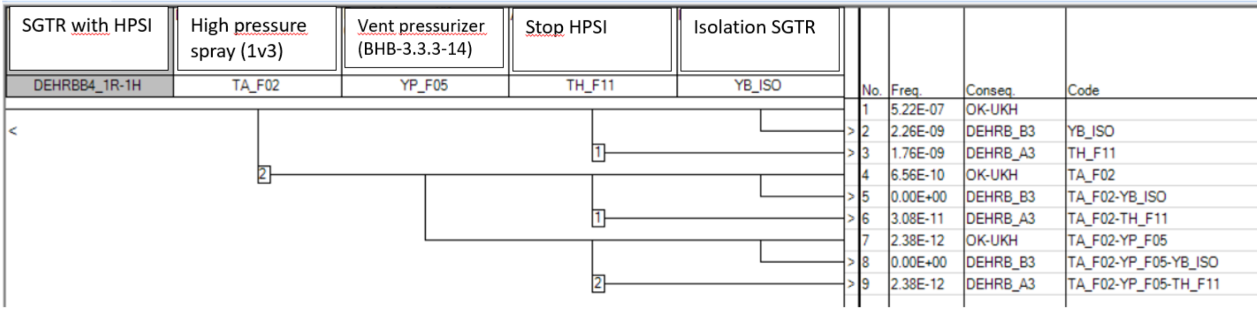
On-site OAs are carried out by plant operators who are aware of the scram that has taken place, but who have no precise idea of the plant's condition. The plant operators are not put under any particular time pressure or stress when carrying out EOP OAs, so nominal stress (SF = 1) is applied for on-site measures from the EOP. For OAs from the SAMG, it is assumed that the plant operators recognize the seriousness of the situation, so increased stress (SF = 2) is applied here. If the OA is to be carried out under difficult conditions, for example in rooms/compartments with a higher dose rate, or if the criteria for the general alarm "Serious Emergency - S" have been met, extreme stress (PSF = 5) is applied.
Various recovery factors are being also applied in order to weigh in the relative difference between the EOP OAs directed by white chapters and the ones directed by black chapters. Namely, given the highly structured form of both the white and black chapters and in accordance with the rationale on page 15-15 from reference [1], in case of the EOO a recovery factor of 0.33 is applied. On the other hand, a multiplier of 2 for the stress factor is used given the error of commission in case of application of the white chapters, as a way of relativization vis-à-vis the case of applying the black chapters (long versions) of the OAs.

The ESD also show the different conditions an operator action is used for. By defining the relevant operator actions of a sequence, the ESDs also clearly outline potential HRA dependencies between/among operator actions and support the quantification of their dependencies. Such an assessment of dependencies between/among operator actions is also required by the Swiss nuclear regulator. The quantification of operator action dependencies is presented in [3].

4. Development of the event trees (ET) in the PSA model

The event trees in the PSA model base directly on the IE-ESD. The blocks of the IE-ESD are used as functional events in the ET. The transfer gates of the IE-ESD are also used as transfers from one event tree to the next event tree. In this way, the ET structure is easy to develop and understand. RiskSpectrum® PSA is used to model the PSA. This software allows to link event trees to other event trees, making the overall structure of the sequences easier to trace and understand. On functional event level, different alternatives can be distinguished. With this feature, different conditions developed in the IE-ESD can be nicely represented and modelled in the event trees. To trace the different linked ET of an initiating event, the names of the IE-ESD transfers are used.

Figure 4 below shows the event tree representing the IE-ESD from Figure 2. As can be seen, the ET start with an event representing the condition, here it is a SGTR with HPSI running. Other functions like SCRAM, turbine trip, secondary feed water system and steam relief are challenged in previous ETs linked to this one.



	No.	Freq.	Conseq.	Code
	1	5.22E-07	OK-UKH	
>	2	2.26E-09	DEHRB_B3	YB_ISO
>	3	1.76E-09	DEHRB_A3	TH_F11
	4	6.56E-10	OK-UKH	TA_F02
>	5	0.00E+00	DEHRB_B3	TA_F02-YB_ISO
>	6	3.08E-11	DEHRB_A3	TA_F02-TH_F11
	7	2.38E-12	OK-UKH	TA_F02-YP_F05
>	8	0.00E+00	DEHRB_B3	TA_F02-YP_F05-YB_ISO
>	9	2.38E-12	DEHRB_A3	TA_F02-YP_F05-TH_F11

Figure 4. ET based on ESD from Figure 2

As in this part of the event tree secondary heat removal is already available, block 46a has not to be asked again.

A great help in developing the IE-ESD was the plant specific accident simulator MELSIM® [4], which is based on MELCOR [5]. MELSIM has, among many other features, an interactive GUI allowing directly interacting with the running MELCOR simulation. The deck is detailed enough to also be used for simulating success criteria for the PSA. About 200 simulations have been run to distinguish various core damage and success conditions for a broad range of LOCAs, steam generator tube ruptures, containment bypass LOCAs and transients. A database structure has been developed together with a small program to automatise report generation of these simulations.

5. Using the PSA model

After modelling the event tree and fault trees in RiskSpectrum® PSA, the PSA model can be used to analyze potential plant modification to reduce the risk. One such study focusses on reducing the risk posed by a stuck open SG safety valve given SGTR. Main contributors to stuck open SG safety valves are sequences where secondary depressurization using the SG relief valves is not fast enough (operator action) and sequences where the HPSI pumps lead to overfilling the SG with the ruptured tube. Thus, one plant modification addresses an automatization of the opening of the SG relief valves to limit pressure below the set point of the safety valves, the second plant modification addresses limiting the pressure of the HPSI pumps for SGTR events.

5.1 Automatization of SG relief valve opening

Currently the SG relief valves are opened by an operator action from the main control room. Existing signals of the turbine bypass system could be used to generate a new signal to open these valves. In this way, the existing operator action would be not required and only be a backup to the new signal anymore.

The new signal is included in the module for steam relief using the SG relief valve and the event tree structure for SGTR required no changes. The SGTR event tree was copied and the functional fault tree for SG relief valve was replaced with the new one which includes the automatic opening of SG relief valves.

In the PSA model, a new consequence analysis case was set up and the model could be quantified. The plant modification would reduce CDF contribution of SGTR by 4% and LERF contribution of SGTR by 3%.

This will also impact the assessment of other operator actions in the sequence, as dependency between operator actions are modelled.

5.2 Limiting HPSI pressure

Limiting HPSI pressure for SGTR events is more difficult a change. A bypass system could be installed opening in case of SGTR events and therefore limiting injection pressure of the HPSI pumps to a value below the pressure set point of the SG safety valves. Feasibility studies regarding this plant modification are ongoing. The probabilistic assessment of this modification includes the following:

- Identification of the sequences which can benefit from this modification.
- Assessment of operator actions and their time windows impacted by this change.

No new event tree structure was developed to reflect the new plant behaviour. Instead, the HEP for the operator action currently used to stop HPSI was divided by 3 for the corresponding sequences. This should lead to a reasonably good estimation for the risk reduction, and cover the failure probability of the signal and the required hardware function (opening of a valve).

The following changes in the PSA model were conducted:

- Setting up a new consequence analysis case for all three different sizes of SGTR (double break of 1 tube, double break of 2 tubes, and double break of up to 5 tubes).
- Defining new boundary condition sets to set the operator action for stopping HPSI to guaranteed success in the relevant sequences.

As the time window for the operator action to stop the HPSI pumps decreases with increasing number of broken tubes, the relative risk reduction increases with increasing number of broken tubes.
In all, the quantification shows that the pant modification would reduce CDF contribution by SGTR 27% and LERF by 30%.

6. Conclusion

This paper presents the development of the Event Sequence Diagrams as a crucial part of the development of a new plant-specific, full-scope industrial-scale L1/L2 PSA-model for KKG NPP, Switzerland.
The most important applications of these ESDs are the presentation of the overall structure of the plant behaviour, documenting the PSA-relevant functions of the plant, helping the discussion between PSA- and system engineering expert and reactor operators, defining the basis for developing and documenting the event trees, defining the sequences and conditions for the assessment of human error probabilities for the various operator actions,

Acknowledgements

The first and corresponding author is grateful to his colleagues from NPP Goesgen-Däniken AG who provided insights and expertise that greatly assisted the project development. The author also thanks the management of NPP Goesgen-Däniken AG for supporting the PSASPECTRUM Project.

Disclaimer

The views, assumptions, opinions and analysis expressed in this article are those of the authors and do not necessarily reflect the official policy or position of their employer (NPP Goesgen-Däniken AG).

Abbreviations

Abbreviation	**Description**
EOC	errors of commission
EOO	errors of omission
EOP	emergency operating procedures
ESD	event sequence diagrams
ET	event tree
HEP	human error probability
HPSI	high-pressure safety injection
HRA	human reliability analysis
IE	initiating events
IE-ESD	ESD for initiating events
KKG	NPP Gösgen-Däniken AG
OA	operator actions
POS	plant operating states
PSF	performance shaping factor
RPS	reactor protection system
RSHRA	RiskSpectrum® HRA
SAMG	severe accident management gui
SF	stress factor
SGTR	steam generator tube ruptures
THERP	Technique for human error-rate prediction
TRC	time reliability correlation

The views, assumptions, opinions and analysis expressed in this article are those of the authors and do not necessarily reflect the official policy or position of their employer (NPP Goesgen-Däniken AG).

References

[1] Swain A. D. and Guttmann H. E. (1983) Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application. U. S. NRC NUREG/CR-1278.

[2] RiskSpectrum® HRA, Version 1.0.0.4, Copyright © 2013, Scandpower AB.

[3] Kancev D., et al. (2024) Risk Spectrum HRA And Conditional Quantification Tools: Practical Plant Specific Implementation. ESREL 2024 Conference, 3. – 27. June 2024, Krakow, Poland. European Safety & Reliability Network.

[4] MELSIM_KKG Model Documentation for MELCOR 2.2, RMA-KKG-045, Rev. 3b, Risk Management Associates, Inc., 1421 Hymettus Avenue, Encinitas, CA 92024, USA

[5] MELCOR 2.2, Sandia National Laboratories, Albuquerque, NM 87185-0748, 2021