Development of a new plant-specific, full-scope industrial-scale L1/L2 PSA-model with the application of the new *RiskSpectrum® Model Builder* Tool

Dusko Kancev[a], Gerben Dirksen[b], Rainer Hausherr[c], Heiko Kollasko[d], Artem Shevchenko[e] and Christine Bell[f]

[a] NPP Gösgen-Däniken AG, Kraftwerkstrasse CH-4658 Däniken, Switzerland, dkancev@kkg.ch
[b] Framatome GmbH, Paul Gossen Str. 100, 91052 Erlangen, Germany, gerben.dirksen@framatome.com
[c] NPP Gösgen-Däniken AG, Kraftwerkstrasse CH-4658 Däniken, Switzerland, rhausherr@kkg.ch
[d] Framatome GmbH, Paul Gossen Str. 100, 91052 Erlangen, Germany, heiko.kollasko@framatome.com
[e] Framatome GmbH, Paul Gossen Str. 100, 91052 Erlangen, Germany, artem.shevchenko@framatome.com
[f] Framatome GmbH, Paul Gossen Str. 100, 91052 Erlangen, Germany, christine.bell@framatome.com

Abstract: This paper addresses the development of a new plant-specific, full-scope industrial-scale L1/L2 PSA-model at the NPP Goesgen-Däniken (KKG), Switzerland with the main focus aimed at the application of the new *RiskSpectrum® Model Builder Tool*. KKG, together with their supplier Framatome GmbH, embarked on the substantially thorough project – *PSASPECTRUM* – of migrating the KKG`s existing PSA model from *Riskman* to *RiskSpectrum* environment. The first phase of this project encompasses the modelling of internal events, full power, low power and shutdown states for both Level 1 PSA and Level 2 PSA. The system modelling, performed using the *RiskSpectrum® Model Builder* tool, as a part of the *RiskSpectrum®* product family, will be addressed in detail within this paper. This tool facilitates the PSA modelling on system level and is based on a similar tool – KB3 – developed and used by EDF. It is the first full-scope application of *RiskSpectrum® Model Builder* worldwide, excluding the KB3 applications already performed by EDF. The paper will summarize the system modelling strategy applied within the *PSASPECTRUM* project when using the *RiskSpectrum® Model Builder* through several plant system models examples. At the beginning, the different steps from the development of the KKG-specific knowledge base in Figaro language, via the system analyses and creation of FMEA database are discussed. Further on, the steps of the compilation of simplified system P&IDs, their import in the *RiskSpectrum® Model Builder* to the development of the *RiskSpectrum® Model Builder* system models with the end goal of creation of the corresponding fault trees and their export to the plant-level PSA modelling, i.e., linking within the event tree structure in *RiskSpectrum® PSA* environment, are presented. The conclusion of the paper summarizes the great advantages of using this new tool, mainly due to the guaranteed systematization of PSA modelling as well as the simplification of quality assurance and model maintenance in future.

1. INTRODUCTION

In July 2020, the NPP Gösgen-Däniken AG (KKG) launched a new project (*PSASPECTRUM*) of refurbishment and restructuring of its plant specific PSA model in a new software environment and using new software tools. The main purpose of this project is the progression of the current KKG PSA model into the *RiskSpectrum®* software suite, including its update in terms of consideration of all the additional plant modifications, model & documentation review, necessary model & documentation corrections, increasing the level of modelling detail as well as improving the level of modelling and documentation consistency. Hence, with the *PSASPECTRUM* project, KKG will achieve a consistent and comprehensive PSA model and documentation, compiled within a state-of the-art PSA modelling software environment, allowing to perform the relevant PSA applications and to fulfil the national regulatory requirements more effectively and in a more efficient manner.

The goal of this project is to produce a full-scope, all plant operating states (POSs) (full-power, low power & shutdown), all IEs classes (internal & external), all hazards (internal & external), fully coupled (L1, L1+, L2) plant model.

One of the main highlights of the project is the application of the *RiskSpectrum® Model Builder* (RSMB) tool on the system level PSA modelling. The RSMB is a software tool for building and maintaining risk-, reliability and availability models. Building on the strength of KB3 [1, 2, 3], originally developed and used by Électricité de France SA (EDF) for risk analysis across their critical infrastructure, RSMB, accelerates the generation of risk and reliability analysis by automating and standardising the risk modelling process. By using this platform, EDF has experienced productivity gains of 40-80%. As such, the RSMB [4, 5] was commercialized by Lloyd`s Register RiskSpectrum AB in 2019/2020 and rendered compatible with the RiskSpectrum PSA platform as part of the RiskSpectrum suite.
The three key features of the RSMB tool are improving the automation, acceleration and the standardisation of the risk and reliability modelling process:

- Intuitive drag-and-drop interface to draw systems and subsystems based on the actual P&IDs;
- Central knowledge base containing standardised definitions of systems, structures and components (SSCs) as well as their functional properties and constraints.
- Automatic generation of fault trees and other risk models for each system design, with automatic export into RiskSpectrum PSA ready for further analysis and/or PSA-modelling further on, on the plant-level.

The application of the tool offers higher grade of consistency in the PSA studies; The modelling assumptions are systematic and traceable and a higher grade of homogeneity among the system models is achieved. Also, once the PSA model is built by using the RSMB tool, then a rapid, efficient and systematic model update potential is ensured for the future.

This paper presents a summary of the system-level PSA modelling using the RSMB tool within the framework of the *PSASPECTRUM* project. A new method for FMEA analysis developed by Framatome, as presented in [6], based on the PSA-relevant systems` P&IDs, is presented as the first step of the system-level PSA modelling. Each of the relevant systems P&ID is screened for PSA-relevant components, which are in turn then marked in a way that is reflecting their corresponding failure mode relevant for the analysed PSA system function. These pre-formatted P&IDs are then used as the basis for building the corresponding system function availability models with the RSMB tool. In this regards, three different systems are presented within this paper as case studies – the emergency core cooling system ECCS (TH), the start-up and shutdown feedwater (FW) system (RR), as well as the conventional closed cooling water system (VH) as one of the important support systems. Each of the automatically generated fault trees (FTs) to the corresponding system functions is subsequently discussed. FT automatic export to the main plant-level PSA-modelling environment, the *RiskSpectrum PSA*, is then demonstrated and FTs binding in the corresponding event tree (ET) discussed.

In summary, this study underlines the need for and importance of a systematic, homogeneous, traceable and easily validatable approach with a minimal potential for human errors when developing a PSA-model in industrial-scale projects.

2. MODELLING STRATEGY

This chapter presents the various steps, undertaken in the course of the modelling strategy we have implemented for the application of the RSMB as an add-on in the *PSASPECTRUM* modelling chain component-level → system-level → plant-level modelling.

2.1. Creation of Knowledge Base

The development of a plant-specific knowledge base (KB) by Framatome was the first step towards the implementation of the RSMB tool. A plant-specific KB encompasses the various components that are to be considered by the system modelling. For a category of systems (thermohydraulic systems, electrical systems, etc.), each class is identified by a name and contains a series of characteristics which

are common to the components it describes. This is coded with the *Figaro*-language in the *jEdit* environment (right-hand side of Figure 1). A Figaro-KB therefore contains a description model common to all the systems in the category. Further on, each object in a system belongs to a class (left-hand side of Figure 1). Each object in the system is created as an instance of a class in the KB.

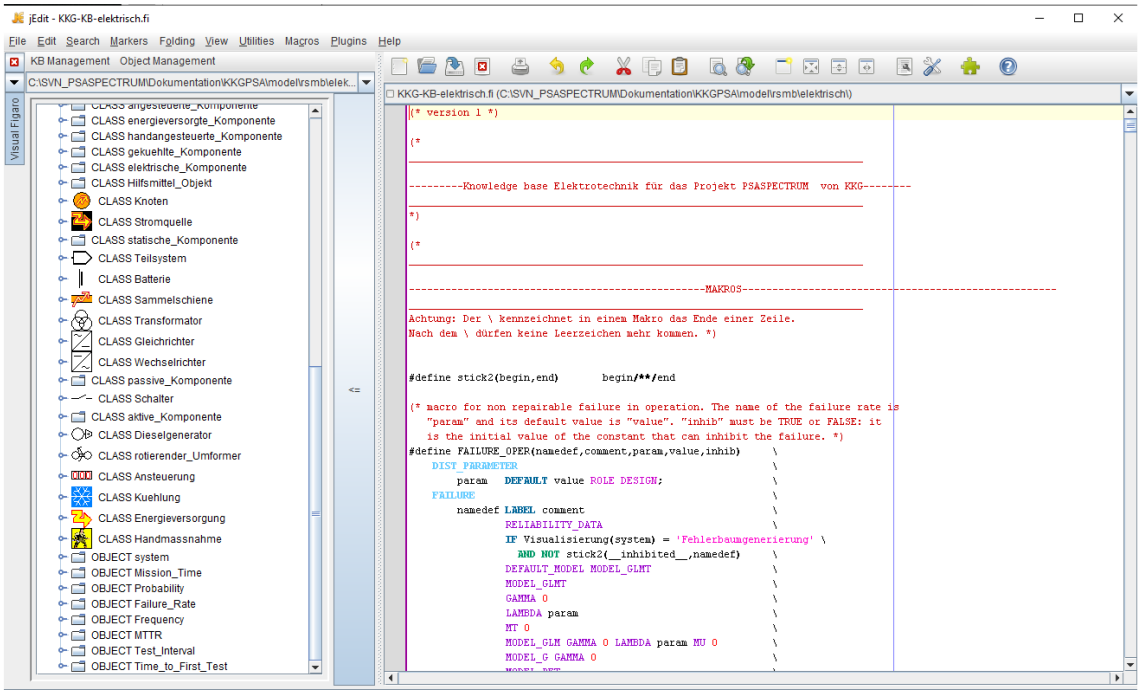

Figure 1: Snapshot of the KKG`s electrical KB

In the course of the creation of the two KKG KBs (one for hydraulic and one for electric systems), the components boundaries were aligned with those according to the German Centralized Reliability and Events Database (DB) (ZEDB - *Zentrale Zuverlässigkeits- und Ereignisdatenbank*) [7]. The two compiled KBs as well as the project in general, are compiled in German.

2.2. FMEA, identification and editing of PSA-relevant P&IDs

After compiling the KB, the different systems are analysed in the next step. Relevant plant systems are designated and their PSA-relevant functions are identified. Each system`s piping and instrumentation diagram (P&ID) is used as an input, i.e. pattern in the process of compilation of the corresponding RSMB-model. A separate pre-edited P&ID is dedicated to each PSA-relevant function of a given system. The components of such a P&ID are marked with different colours (example in Fig. 2: green – fail to open/start & run; blue – passive integrity loss/leakage; light blue – spurious close; pink – spurious open) according to an agreed convention corresponding to the different components` failure modes. This step is also a parallel step of the FMEA for a given system. A FMEA-DB is being created for each analysed system, which is also in alignment with the marked P&ID. Framatome's dedicated software tool ("*ScanAKZ*", see also [6]) enables the automatic import of the marked P&ID to the FMEA-DB.

Fig.2 presents a part of the marked P&ID of the start-up and shutdown FW system (RR) for the PSA-relevant function of this system (in the event of loss of offsite power, failure of the main feedwater (MFW)-pumps and also in the event of pipe ruptures in the water-steam circuit, to ensure the secondary side feedwater input to steam generators (SGs) from the FW- tank). Using another dedicated script, KBMassImport, also specially written by Framatome in the course of the *PSASPECTRUM* project (see also [6]), a KB input file is automatically created which allows for a so-called automatic mass import of the FMEA-DB for the given system into the RSMB (Fig. 3). The FMEA-DB is designed as a comprehensive relational database using the Microsoft Access DB platform. The following information

is stored within the FMEA-DB: component plant ID, component type & description, system affiliation, relevant system function, relevant failure mode for the given system function, relevance for the PSA, intra and inter-system dependencies, power supply and related I&C, cooling, allocation of the common cause component group (CCCG).

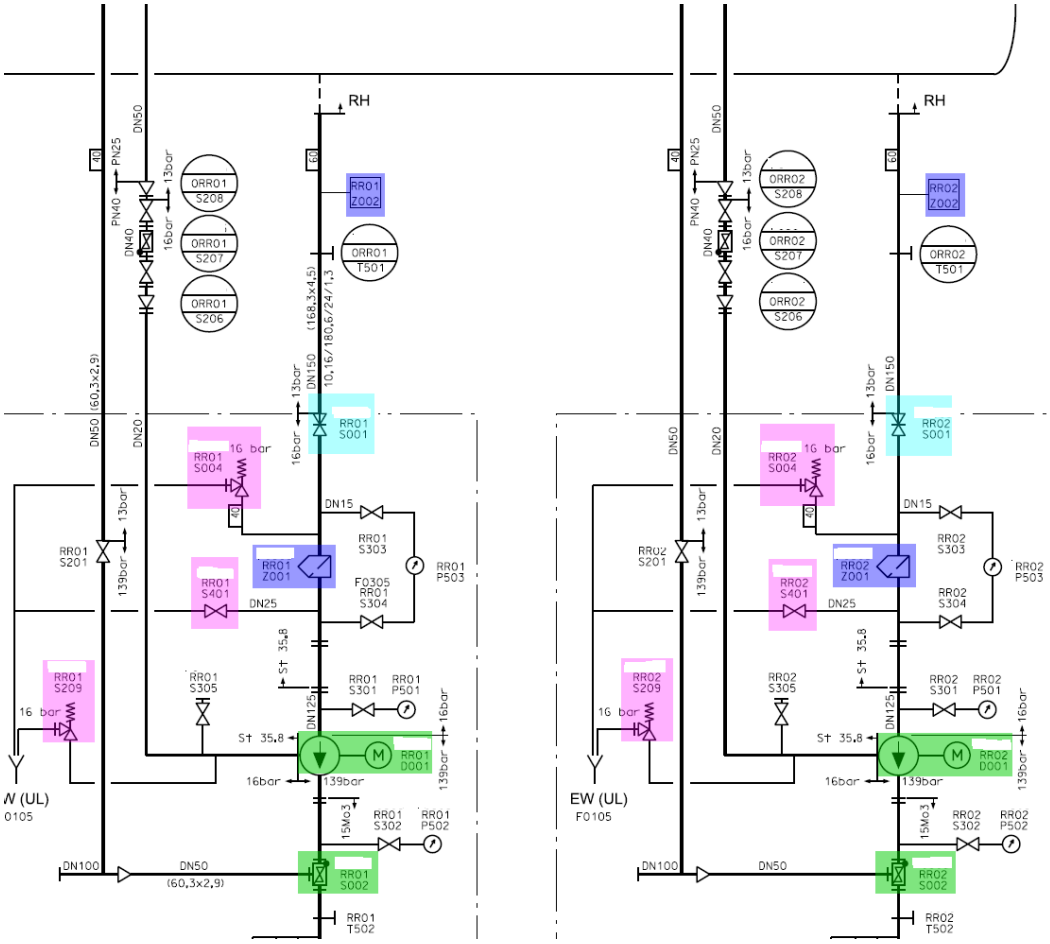

Figure 2: Part of the RR-System – marked P&ID according to colour convention

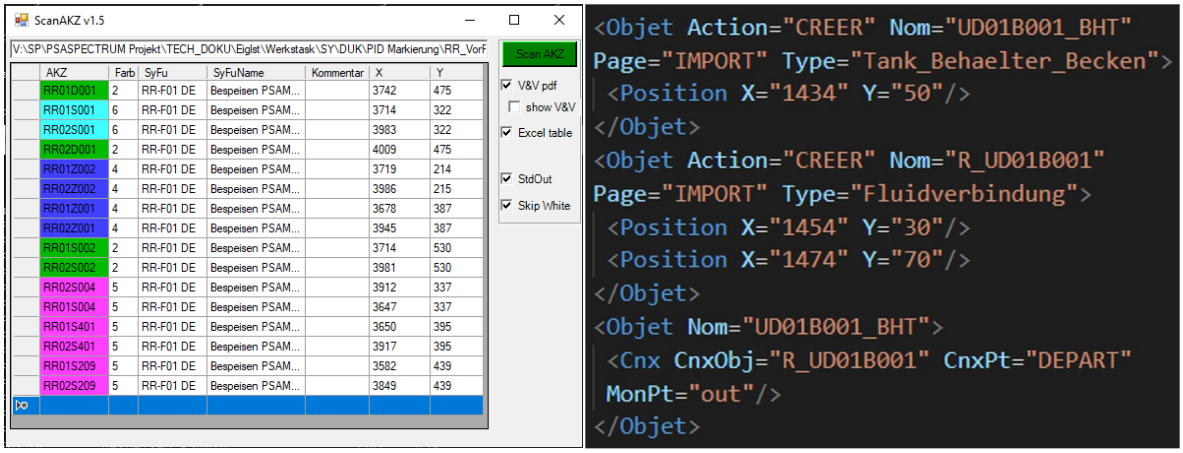

Figure 3: "ScanAKZ" for the RR-System (left side); "KBMassImport" Script (right side)

As mentioned above, the marked system P&IDs form the basis for the FMEA.
The marked system P&IDs are being read-in into the FMEA database with the help of the "ScanAKZ" tool. Firstly, all components that are not required for any PSA-relevant system function are not

considered further. Subsequently, a screening is carried out for the components marked in a PSA-relevant system function. The following figures present parts of the FMEA-DB for the ECCS (TH).

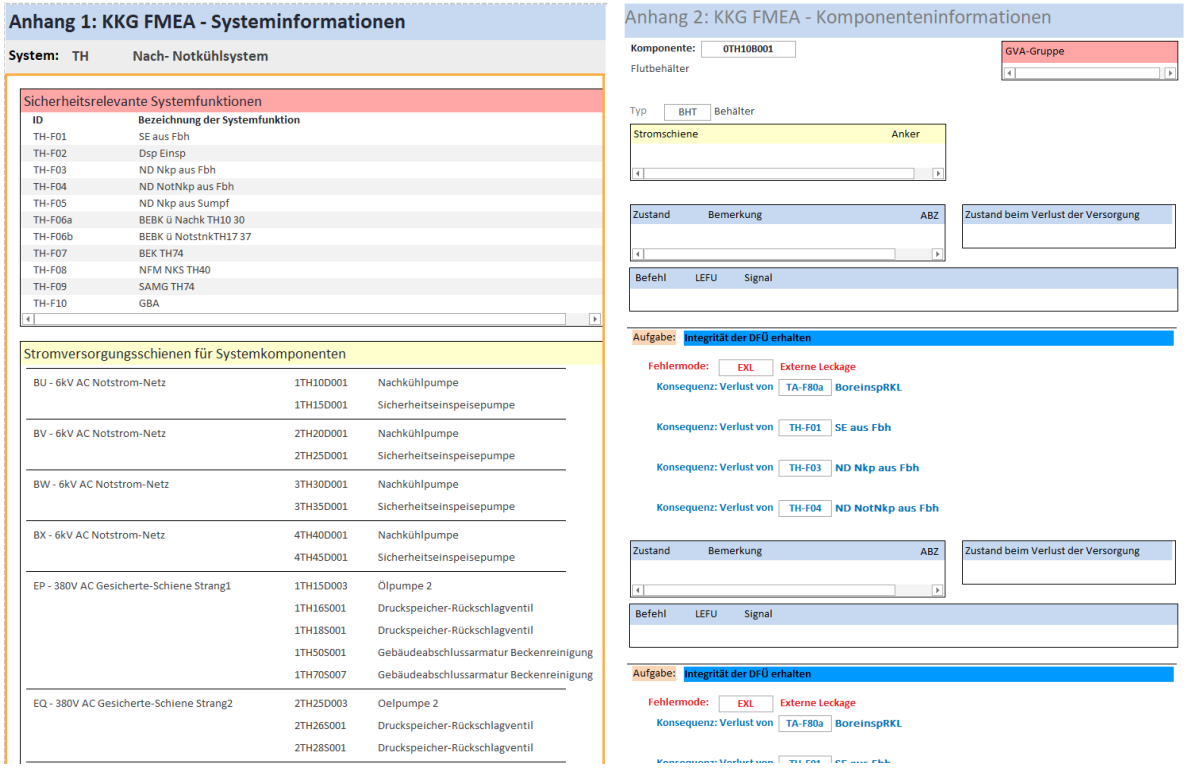

Figure 4: FMEA TH-System information (left side); Component information (right side)

2.3. Creation of a RSMB Model

A RSMB-study is created for each system. The subsystems are divided into "graphic macro components". This can be done per system train, per system function or per subsystem. The subsystems are each shown with a simplified system circuit diagram. In addition, the support systems (external system references) are collected separately in a graphical macro component.

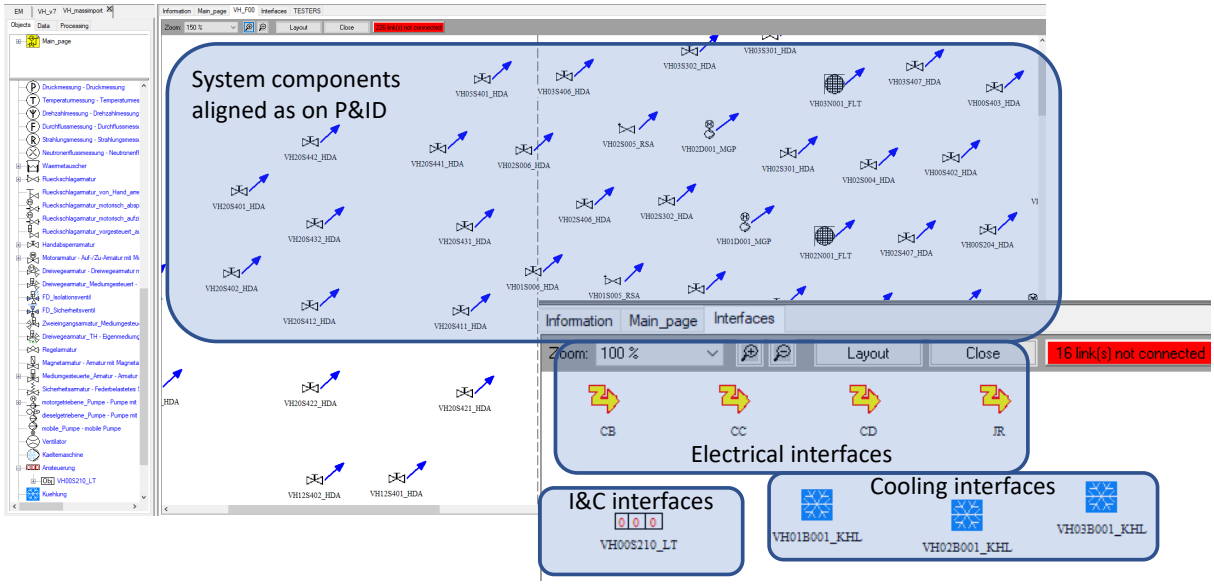

Figure 5: Example result of the automatic import using the tool "*Mass Import*" – VH System

By using the "*Mass Import*" tool, all the components marked in the P&ID are imported in the RSMB environment with all their FMEA-characteristics and at the same "geographic" position on the canvas as their coordinates in the source P&ID (Figure 5). this simplifies building the RSMB model.

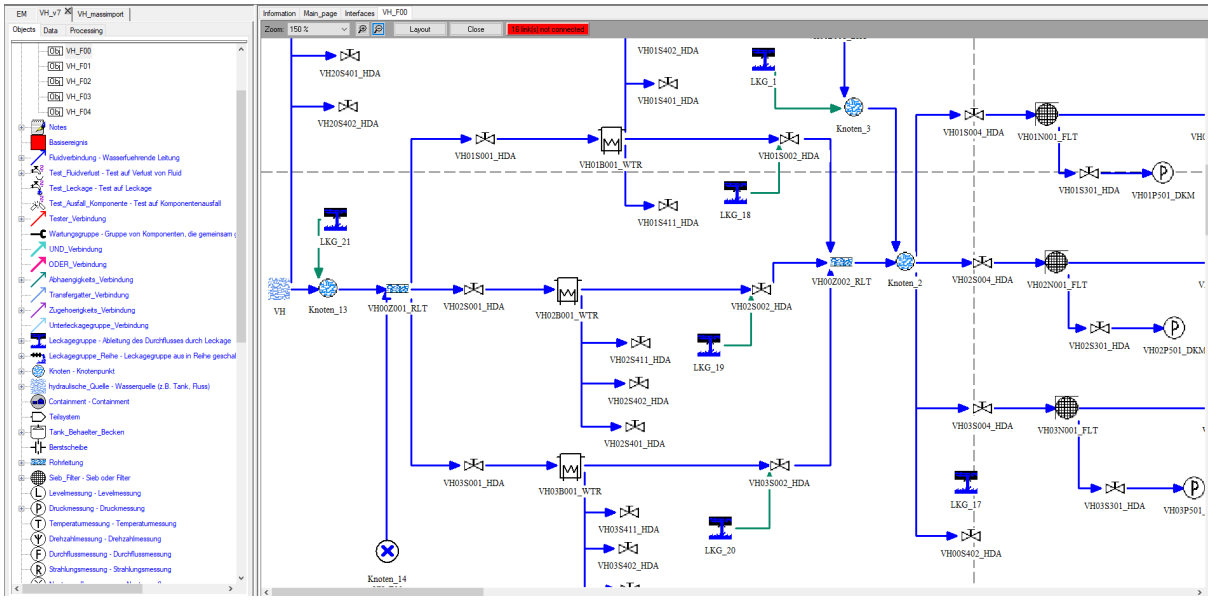

Figure 6: Part of the RSMB model of the VH System

So, basically the system drawing is created based on the available components and links within the KB on the left-hand side of the canvas panel. Characterization of components in terms of the initial state and mission state may be different depending on different system functions. To cope with this within the same RSMB study, RSMB allows for the definition of different system configurations. This is being done by defining various profiles ("VH_F01" - blue color in Fig. 7), or different variants within the same profile ("VAR_VH12", "VAR_VH13", "VAR_VH23" - magenta colour in Fig. 7). Several drawings can be defined on the same page.

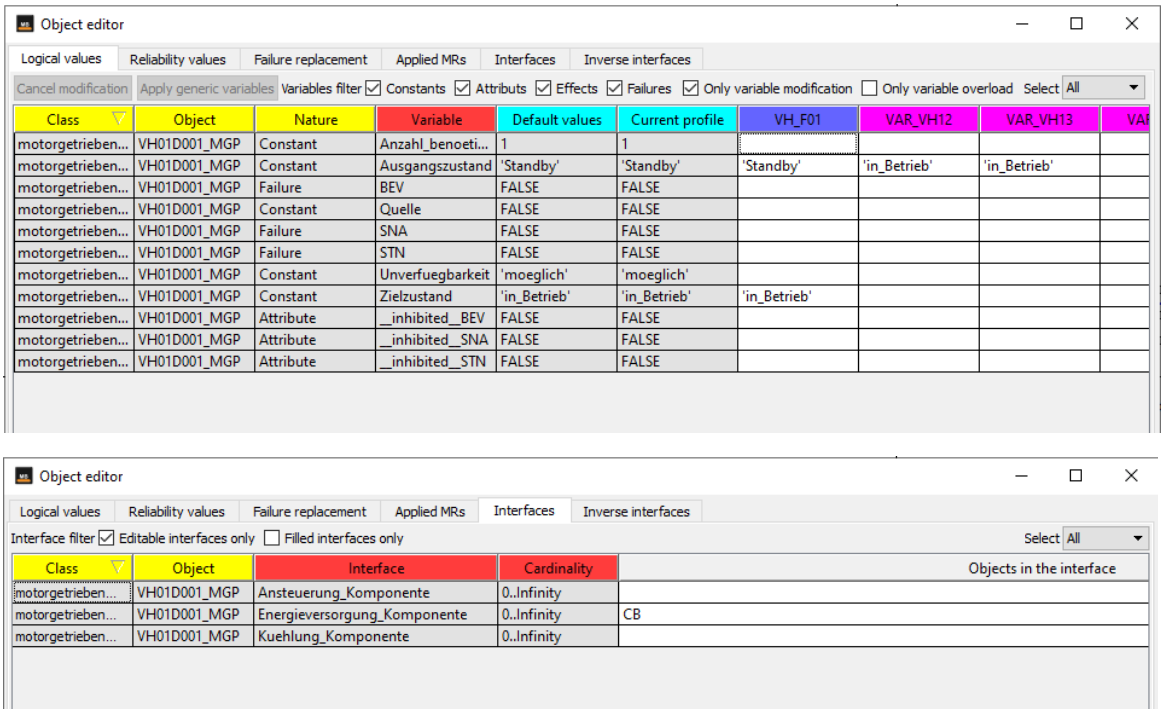

Figure 7: Automatic import of component states and dependencies

Links can be added graphically or through interface. Here this is shown through interface for the power supply of the motor driven pump in the conventional intercooling circuit system (VH) – VH01D001 (Fig.7). The "*Mass Import*" tool accommodates also for the option of automatic import of the different component states and dependencies, as defined within the FMEA database.

2.4. Definition of the undesired event

After finalizing the RSMB model, one should then define the undesired event (UE) which will correspond to the top event in the exported FT within RiskSpectrum PSA. The UE practically tells the software what are the system failures for which one would like to generate a FT. These UE trees are defined using the same FT logic (OR, AND, K/N-gates) as the FTs within RiskSpectrum PSA. The inputs to the UEs can be:

- System references: "test" of variables in the system structures, depicted through the "testers" (loss-of-fluid, leakage, loss-of-function) as graphical elements comprised within the KB;
- External references: links to a top FT outside the current RSMB system study;
- House events: applied as logical switches similarly as within the conventional FT creation methodology in RiskSpectrum PSA;
- Gates: logical operators to combine the above information (OR-, AND, K/N-gates).

Figure 8 presents the definition of the UE for the modelled RR-system, i.e., for its PSA-relevant function: secondary side water supply of at least one SG using the start-up and shutdown system (RR).

In case there is additional information to be added in the model (not already included within the knowledge base for some reason), "manual rules" can be applied. With the help of such manual rules, one can model e.g., maintenance, loss of minimum flow, backflow, etc [4, 5]. The most current use of manual rule is for assigning a value to a variable already modelled by the KB by conditions concerning variables not considered by the KB.

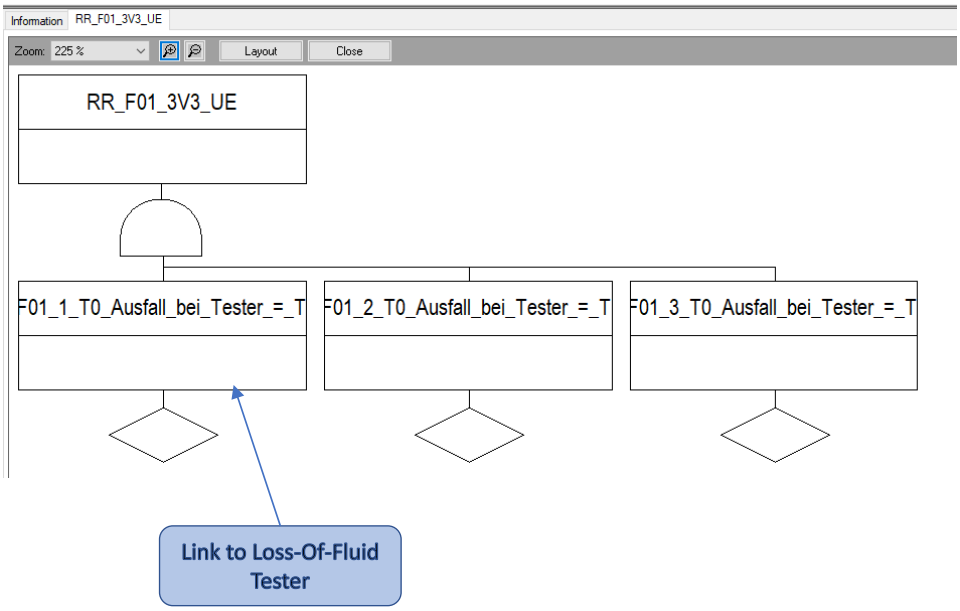

Figure 8: Definition of UE through testers

2.5. Preparation and compilation of the fault tree

After the UEs are defined, one can proceed to the compilation of the corresponding FTs (Fig. 9) within the same RSMB study. The system configuration is defined from a profile (mandatory) and from

variants (optional). The user should select the required system profile, possibly apply variants via house events as a sub-configuration within the same profile or overload those variants into the selected profile (i.e., overriding the configuration`s setting with the one of the variant). Basically, the RSMB tool allows defining different configurations and eventually used in different cases when the FTs are generated.

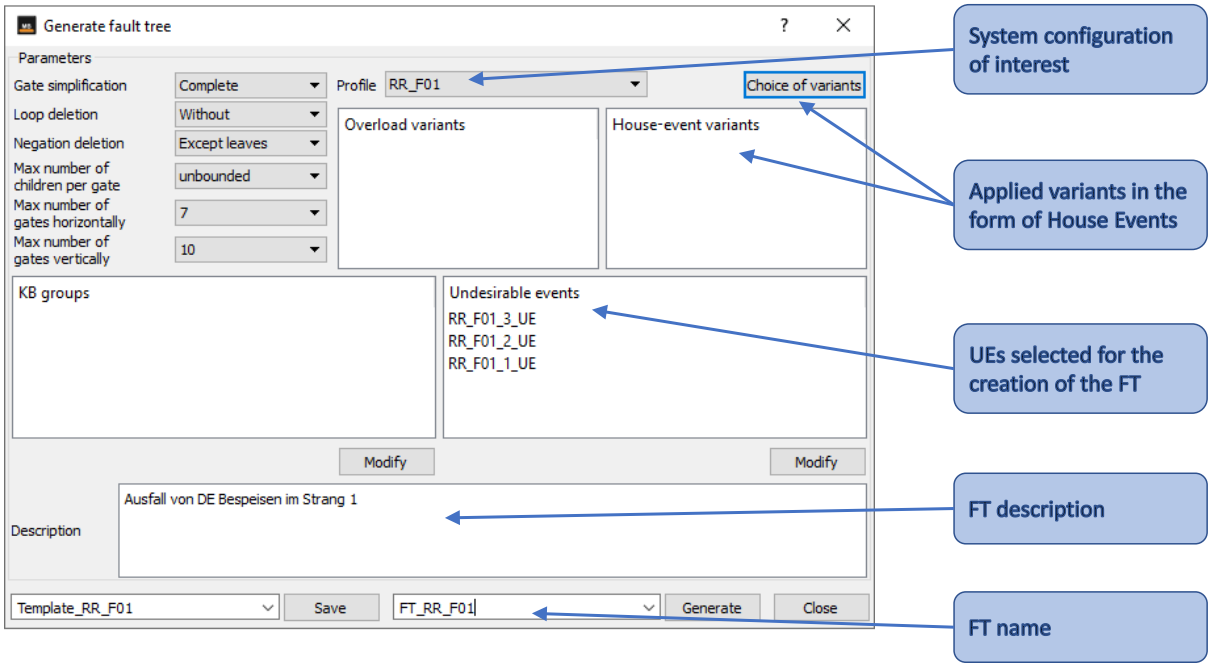

Figure 9: Fault tree generation within RSMB

Another powerful feature of the RSMB tool is the possibility to visualize the configuration of interest. This is one exceptionally important and helpful property for the RSMB model debugging process. The bold blue lines present the undisturbed, uninterrupted inventory (water in this case of the RR system) flow, whereas the red lines represent the mode sections where this flow is being interrupted.

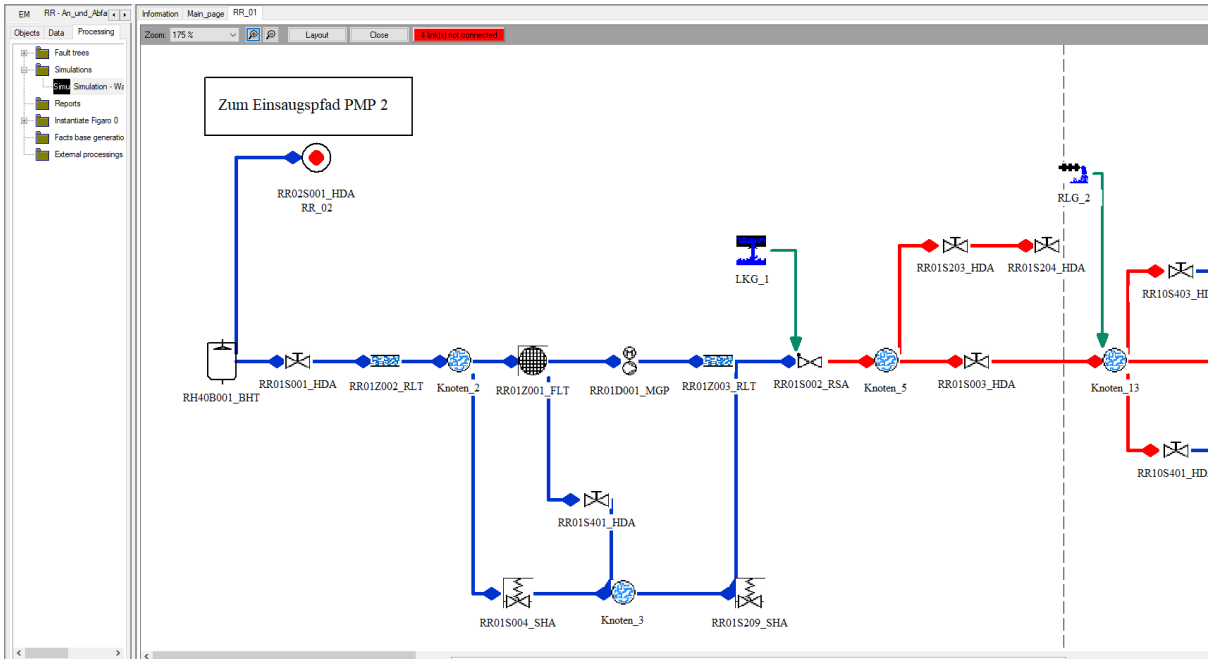

Figure 10: Visualization of a selected configuration – RR System example

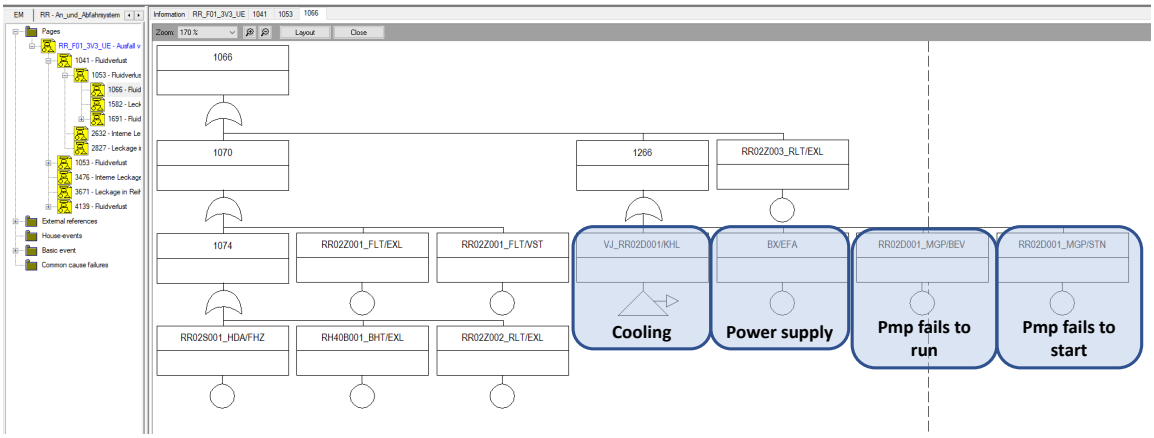

Figure 11: Creation of FT in RSMB – section of the RR-System FT

2.6. Creation and analysis of the fault tree

After the steps, described in chapter 2.4. are performed, the FT is generated within RSMB.

Fig.11 shows a section of the generated FT comprising the logical modelling of the failure probability of one of the RR-pumps. As one can see from Fig. 11, the supporting interfaces (cooling and power supply) are included within the logical structure alongside the random probabilities of pump failure to run and failure to start. The cooling of the RR-pump is performed by another supporting interfacing system – the secured closed cooling water system VJ. In such cases of modelling interfacing systems, the RSMB accommodates for the use of so-called *external references*. External references in RSMB are leaves used in the description of the undesirable events and the manual rules of the study. They refer to a gate of a fault tree in another study [5].

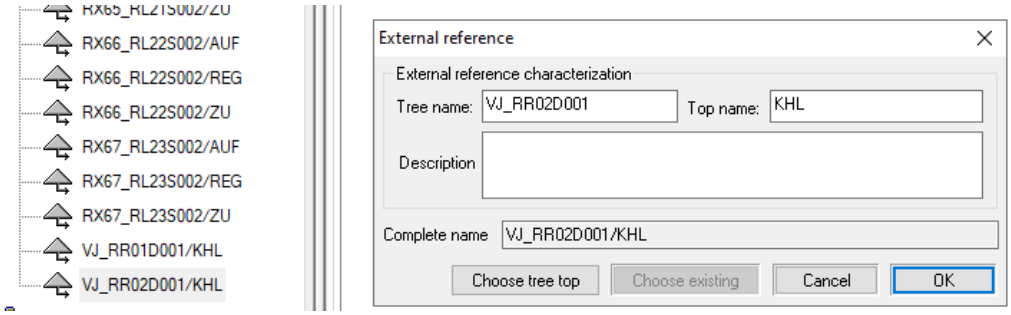

Figure 12: Use of external references in RSMB – cooling of RR/pump with the VJ-system

In other words, the external references are references to pre-defined FT pages, within or external the current RSMB study. The external references are possible to be used as failure replacements. RSMB enables the user to replace failures with other failures or by external references specified by the user in the profile during the generation of a fault tree. The events of replacement are exploitable only in generation of tree such that the failures will be replaced in the FT generated by the event of chosen replacement. In this specific case of the cooling of the RR-pump described above, the external reference VJ_RR02D001/KHL, presented as a FT leaf herein, will be replaced by a FT-subtree, modelling the concerned train of the VJ-system, once the RSMB fault tree is exported to the main RiskSpectrum PSA platform and linked with the other FTs on the PSA plant-level modelling.

2.7. FT export to RiskSpectrum

Once the RSMB study is finalized and the FT generated within RSMB, one can proceed to export the trees to the RiskSpectrum PSA environment (Fig. 13). One can choose which RSMB trees are to be

exported to the RiskSpectrum PSA target project (Fig. 14). Consistent naming of basic events, top gates and intermediate gates is ensured using naming rules (Fig. 13).

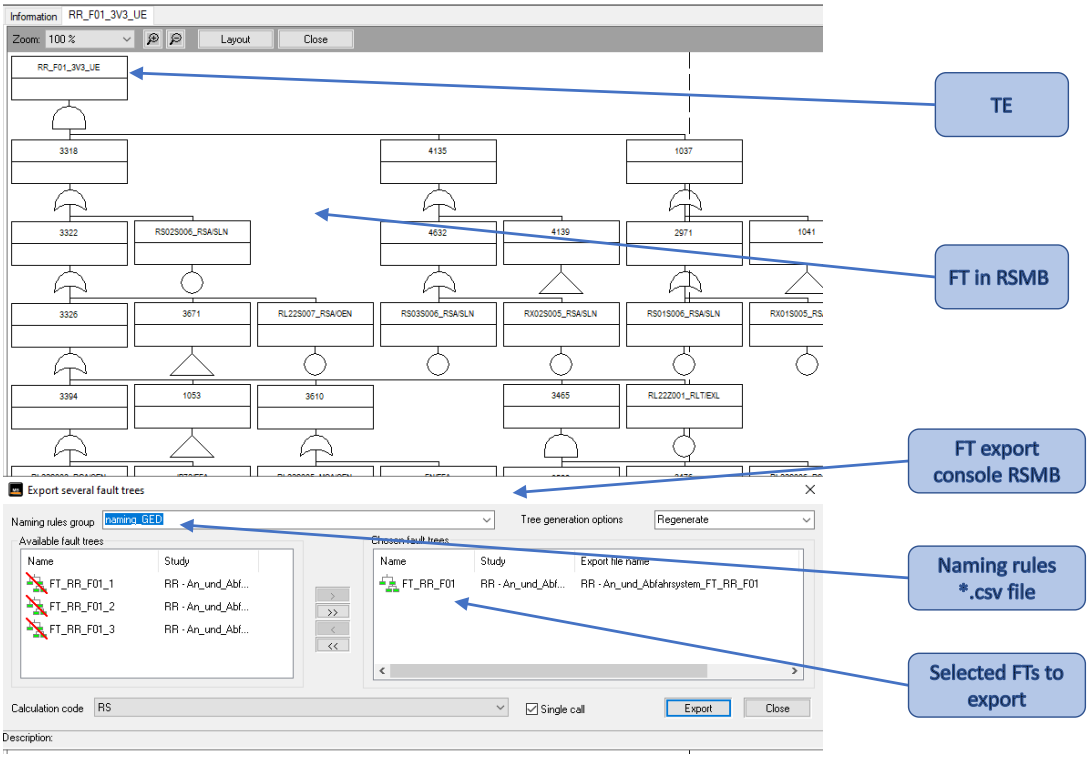

Figure 13: Top event and FT Export console from RSMB to RS PSA – RR system example

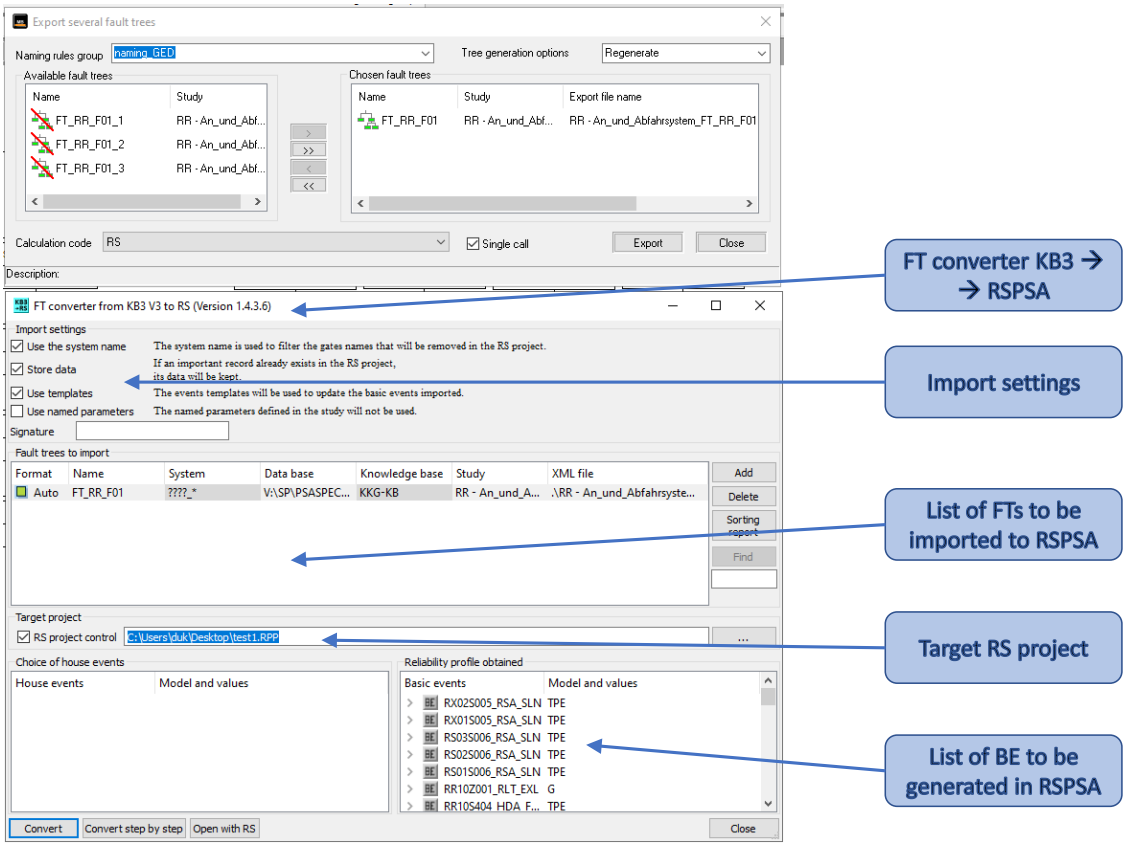

Figure 14: RSMB export console and FT converter (RSMB) to RiskSpectrum PSA

Different import settings (Fig. 14) allow for different helpful options, such as: removing the existing FTs in the target project that are matching the pre-defined naming mask; (non)preserving of existing BEs, HEs, parameters and CCFs; (non)using the parameters defined in the RSMB study. Figure 15 shows the fully-converted FT to RiskSpectrum PSA.

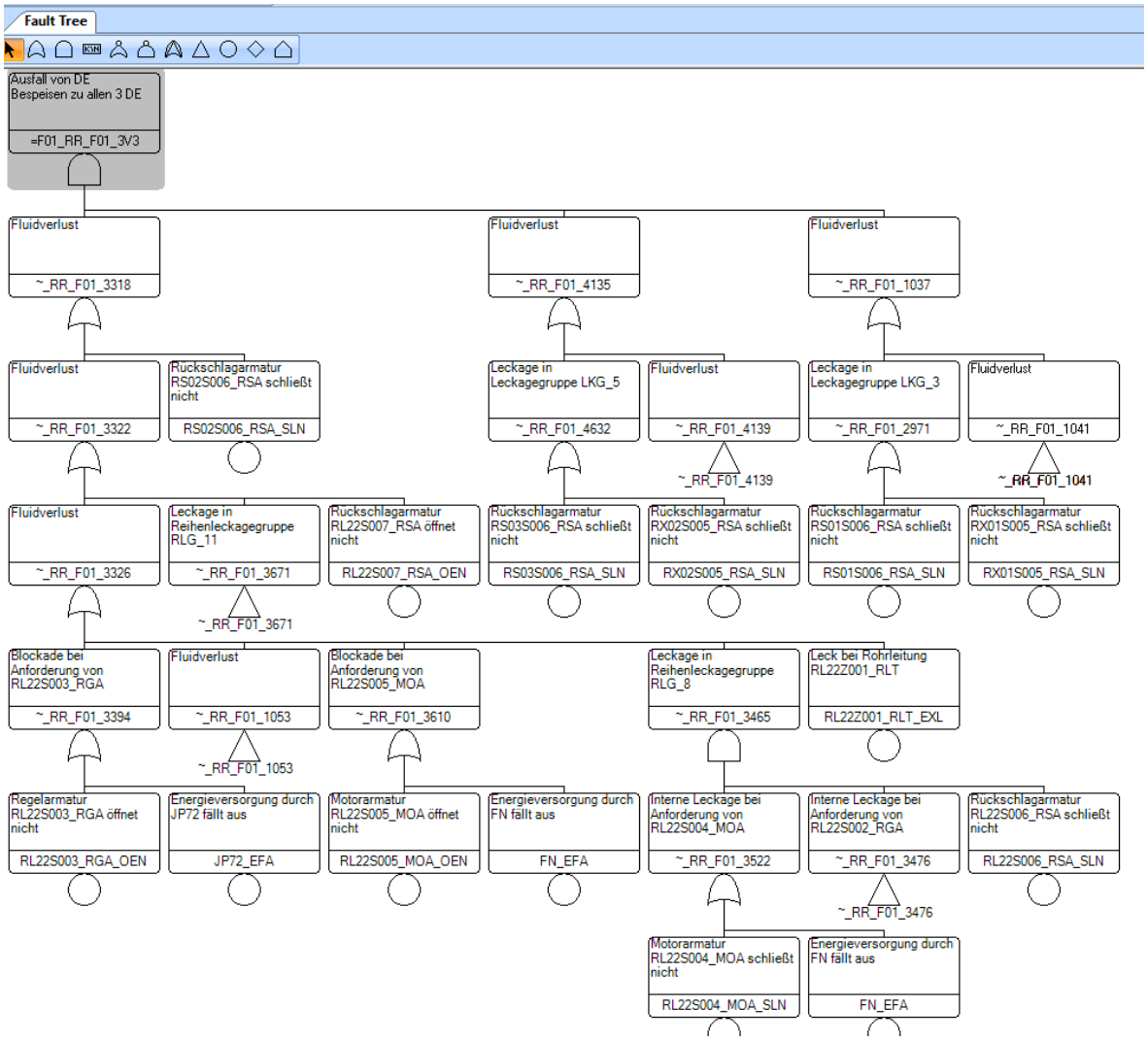

Figure 15: Exported FT to RiskSpectrum PSA – RR system

3. CONCLUSION

This paper presents, in a nutshell, the application of the new RSMB tool 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 features of this tool are: the intuitive drag-and-drop interface to draw systems and subsystems based on the actual P&IDs; the creation and application of central KB containing standardised definitions of SSCs as well as their functional properties and constraints; automatic generation of FTs and their automatic export into Risk Spectrum PSA.

A new system-level modelling strategy is presented, comprising the different steps from the development of the KKG-specific knowledge base in Figaro language via the system analyses and creation of FMEA database, compilation of simplified system P&IDs, their import in the RSMB to the development of the RSMB system models with the end goal of creation of the corresponding fault trees and their export to the plant-level PSA modelling, i.e., linking within the event tree structure in Risk

Spectrum PSA environment. Three different systems are used within this paper as case studies – the ECCS (TH), the startup and shutdown FW system - RR, as well as conventional closed cooling water system VH as one of the important support systems.

The incurred experience in the system-level PSA modelling implicates the need for and importance of a systematic, homogeneous, traceable and easily validatable approach with a minimal potential for human error for a PSA-modelling in industrial-scale projects. All of this could be achieved by using the RSMB tool. By using the RSMB tool in combination with the presented methodology for automatic processing of pre-edited system P&IDs, a clearly documented and traceable connection between the system P&IDs and the plant-level modelling in RiskSpectrum PSA can be established. The simplified P&IDs allow easy manipulation of the FT model. The routines for automated reading of the simplified P&IDs in the FMEA database as well as the automated import of the PSA-relevant components to RSMB highly increase the efficiency. The quality assurance is conducted by comparative analysis of the FMEA database with the generated RSMB models.

The application of the new RSMB tool ensures a higher grade of consistency in the PSA studies, the modelling assumptions are systematic, traceable and easily verifiable. Also, a higher grade of homogeneity among the system models is achieved. In addition, once the PSA model is built by using the RSMB tool, then a rapid, efficient and systematic model maintenance and model update potential is ensured for the future.

Acknowledgements

The first and corresponding author is grateful to his colleagues from NPP Goesgen-Däniken AG as well as Framatome GmbH, 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 Gösgen-Däniken AG, Framatome GmbH).

References

[1] M. Bouissou et al. "*Knowledge Modelling and Reliability Processing: Presentation of the Figaro Language and Associated Tools*", Safety of computer control systems, 1991 (SAFECOMP '91), Trondheim, Norway, 30 October-1 November 1991.

[2] M. Bouissou et al. "*KB3 Tool: Feedback on Knowledge Bases*", European Safety and Reliability Conference ESREL, Lyon, France, March 18-21, 2002.

[3] M. Bouissou et al. "*Reference Manual for the Figaro Probabilistic Modelling Language*", Version E, January 2019.

[4] X. He: "*RiskSpectrum ModelBuilder (KB3) Training*", Lloyd`s Register, October 2020.

[5] Lloyd`s Register: "*RiskSpectrum ModelBuilder (KB3) User Manual*", March 20, 2020.

[6] G. Dirksen: "*Creating a digital twin reliability model using RiskSpectrum ModelBuilder*", *RiskSpectrum*® User Group Meeting, January 26, 2022.

[7] VGB PowerTech e.V., *"Zentrale Zuverlässigkeits und Ereignisdatenbank"*, TW 805-15 – Band 1, December 2014