Modelling of Failures of Multiple Redundant Trains of the Electrical Power Supply System of NPPs in PSA

B. Brück, G. Gänßmantel, A. Kreuser, C. Müller, E. Piljugin, M. Utschick, and J. C. Stiller
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Germany

Abstract: Failures of multiple redundant trains of the electrical power supply system of NPPs have recently received growing attention by the nuclear community. This was triggered by events at several different NPPs where single causes led to such failures, for example at the Byron and Forsmark NPPs. Such phenomena have generally not been modelled in PSAs yet. Therefore, GRS has initiated a research project aiming at a comprehensive and in-depth analysis of events where multiple trains of the electrical power supply system failed (including open phase conditions) and at the development of modelling and quantification methods to include such phenomena in PSAs, and at the exemplary application of these methods. It comprises five interacting efforts: Firstly, a detailed analysis of international operating experience with respect to actual and potential faults affecting multiple trains of the electrical power supply system of NPPs is carried out. Then a detailed dynamic model of the electrical power supply system of a German pressurised water reactor is developed and used for the investigation of the cause and the propagation of such faults. Thirdly, an existing PSA model of a German PWR is extended to allow for the modelling of the phenomena identified in the previous steps, which includes adding relevant equipment not modelled before and new failure modes of equipment already present. The additional reliability parameters and frequencies of initiating events needed to quantify the extended PSA model are estimated. Lastly, the additional failure mechanisms considered in the extended PSA model are evaluated quantitatively.

Keywords: PSA, asymmetrical fault, open phase condition, CCF, electrical power supply system

1. INTRODUCTION

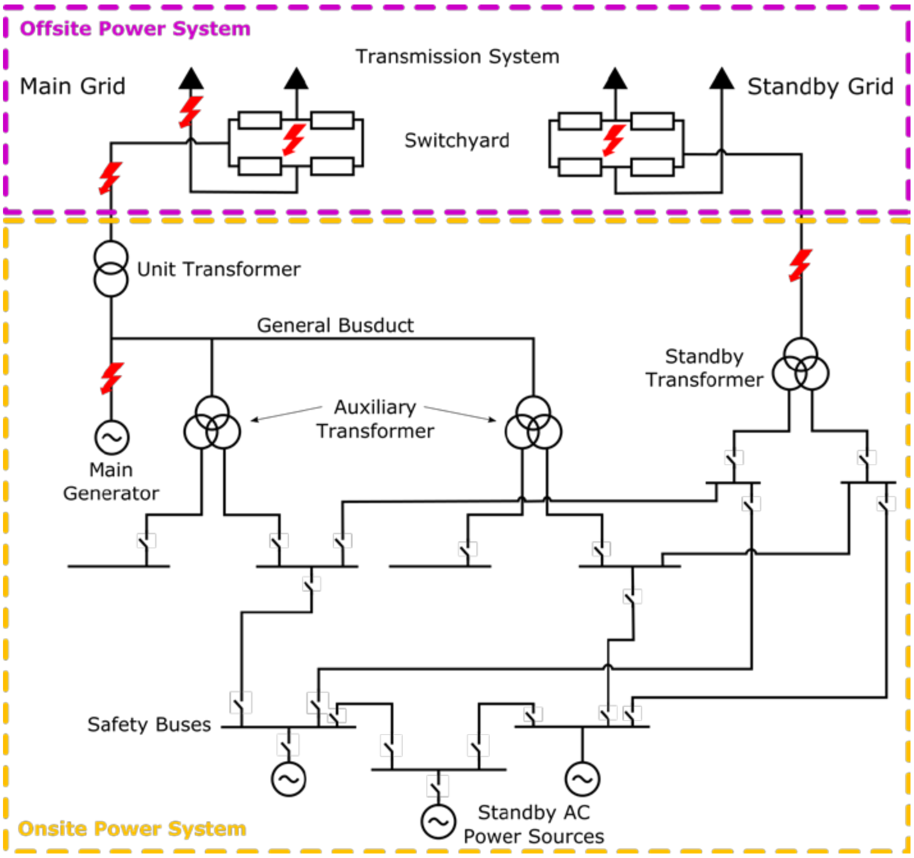
Faults simultaneously impairing multiple trains of the electrical power supply system of nuclear power plants (NPPs) have recently received growing attention by the nuclear community [1]. This was triggered by events that involved so-called asymmetrical faults at several different NPPs where such faults occurred. An asymmetrical fault results from the degradation (e.g. an interruption) of one or two of the three phases in a three-phase alternating current system. For example, at the Byron NPP in the U.S., asymmetries in the power supply system arose from a single failure of an insulator in the switchyard of the plant. The asymmetry failed to cause the reactor protection system (RPS) to initiate the isolation of the emergency bus bars and the operation of the emergency diesel generators. As another example, at the Forsmark NPP in Sweden, the failure of one pole of a breaker to open led to an open phase condition that was also not detected by the RPS. In both cases the electrical consumers remained connected with the fault and were exposed to an asymmetric voltage supply, leading to unavailabilities and even the destruction of electrical equipment.

Such events have generally not been included in probabilistic safety analyses (PSAs) of NPPs yet, which may be attributed to the apparent past general underappreciation of the possible importance of such phenomena. Therefore, GRS has initiated a research project aiming at a comprehensive and in-depth analysis of events characterised by fault states of multiple trains of the electrical power supply system, including – but not limited to – open phase conditions, and at the development of modelling and quantification methods to include them in PSAs.

The electrical power supply system is particularly susceptible to faults affecting multiple trains since during normal power operation there is no separation between the redundant trains. As shown in

Figure 1, failures that occur on or above the generator bus bars will affect all underlying bus bars simultaneously.

Figure 1: Typical electrical systems of a NPP (inspired by [3])



2. STRUCTURE OF THE PROJECT

This project comprises five interacting efforts: Firstly, the possible causes of faults affecting multiple trains of the electrical power supply system and their consequences are assessed from an operating and modelling perspective. To achieve this, initially a detailed analysis of international operating experience is carried out with respect to actual and potential faults affecting multiple trains of the electrical power supply system of NPPs, complementing the analysis of German operating experience with respect to this topic in the course of the general monitoring and analysis of German operating experience by GRS [2].

Secondly, a detailed dynamic model of the electrical power supply system of a generic modern German pressurised water reactor (PWR) has been developed for the investigation of the cause and the propagation of such faults.

Thirdly, a current PSA model of a German PWR is extended to allow for the modelling of the phenomena identified in the previous steps. This includes adding relevant equipment not modelled before and new failure modes of equipment already modelled.

Fourthly, the additional reliability parameters and frequencies of initiating events required to quantify the extended PSA model are estimated. New approaches and procedures to achieve this are developed as needed.

Finally, the additional failure mechanisms considered in the extended PSA model are evaluated quantitatively.

3. OPERATING EXPERIENCE ANALYSIS

The events at the Byron and Forsmark NPPs highlighted the importance of the grid connections and the associated equipment for the reliability of the plants' safety system. These events also revealed the importance of a systematic evaluation and analysis of their operating experience; while the physical and electrical effects that led to the failures were all well-known and well understood in theory, this theoretical knowledge was not used in the design of the safety system of NPPs worldwide until operating experience made these problems obvious.

Therefore, an evaluation of operating experience with a special focus on effects that might impair multiple trains of the electrical power supply system is performed. By doing so, two targets are pursued:
Firstly, the identification of failure mechanisms that might lead to multi-train impairments and that are not yet covered by the design assumption of the plant. Also, events where so far no (multiple) failures have been observed but where the effective failure mechanism may cause such failures in case of other circumstances are relevant.
Secondly, the development of failure scenarios that describe how such failure mechanisms would affect modern German KWU type NPPs. With the development of the scenarios it is intended not only to apply the underlying phenomenon to the KWU type plant, but also to develop variants of the actual event.

3.1. Analysis of events with asymmetrical faults

As a first step, the systematic evaluation of international operating experience with a focus on asymmetrical faults, which was conducted by GRS after the events in Byron and Forsmark, was taken as basis to develop failure scenarios. This evaluation [4] revealed that such faults can be observed regularly in NPP operating experience. Ten events were revealed where the active grid connection of the plant[*], which supplies the consumers, was affected by an asymmetrical fault. In four events such faults were discovered in the standby grid connection. The identified events where active grid connections were affected are presented in Table 1.

Table 1: Events with asymmetrical faults of the active grid

Date	Plant	Failure Cause
1994-05-13	Kalinin	Collapse of a transformer duct, OPC on one phase
1997-02-25	Balakovo	Unintended closure of a single breaker pole
2001-03-31	South Texas	One breaker pole in the switchyard failed to close
2005-11-11	Koeberg	One breaker pole in the switchyard failed to close
2006-07-26	Vandellòs	Mechanical failure of a disconnector
2007-05-14	Dungeness-B	One pole of a HV-transformer breaker failed to close
2012-01-30	Byron	Collapsed insulator caused a line interruption
2012-12-01	Bruce	Mechanical line failure during severe weather (storm)
2013-05-30	Forsmark	Failure to open on command of a single breaker pole
2014-04-27	Dungeness-B	Open breaker pole in the switchyard

The systematic analysis of asymmetric faults showed that a single failure mechanism might lead to various different failure scenarios.

In case of an asymmetrical failure event, the following set of features that had a significant influence on the extent of the degradation of the onsite power system could be identified:

---

[*] The main grid or the stand-by grid may be the active grid, depending on plant state.

- Type of failure: Failures of one and of two breaker poles have been observed in operating experience and need to be analysed.
- Location of the failure: Asymmetrical failures may occur in the main grid connection, the auxiliary grid connection and the generator bus duct, each with different consequences. In case of grid side asymmetries, the different distances between the location of the failure and the plant have to be considered as well as parallel grid connections that are not impaired.
- Neutral point treatment: Operating experience has shown that the treatment of the neutral point of the main or auxiliary transformers has a crucial effect on the propagation of a grid side asymmetry into the plant.
- Load of the onsite power system: Both the load and its characteristics (inductive or ohmic) have an influence on the asymmetry and need to be evaluated carefully.

In total, more than 500 combinations of features can be derived from the list above. Based on the operating experience and engineering judgement with special focus on typical situations in nuclear power plants, 15 potentially relevant parameter combinations were specified. These parameter combinations are given in Table 2. The parameter combinations 1 to 12 constitute a systematic analysis of the failure type (single phase or dual phase failures), the plant condition (power operation and different outage conditions) and the neutral point treatment. The combinations 13 to 15 are used to assess the influence of uncommon failure situations like failures in the electrical grid (meshed or unmeshed) or failures during partial load operation.

All of the parameter sets described above are analysed with the simulation model as described in Chapter 4.

3.2. Analysis of other events effecting multiple redundant trains of the electrical power supply system

Beside the asymmetrical faults, several other phenomena that might affect multiple redundant trains of the electrical power supply system are already known from operating experience, both from the International Reporting System for Operating Experience (IRS) and from German operating experience. Among these phenomena are the Forsmark event of 2006-07-25 [4], where combined voltage and frequency fluctuations in the 400 kV grid caused multiple impairments of uninterruptible power supply (UPS) units necessary for the startup of the emergency diesel generators (EDGs), and an event in a German NPP [5] where four inverters (each in a separate redundant train) failed due to a single failure in a 660 V breaker of a residual heat removal pump. The failure of the inverters may be taken as an example for a CCF due to latent failure mechanism in a continuously running electrical component. These kinds of CCF are in general not modelled comprehensively in PSAs of German NPP.

In the light of these insights it was concluded to extend the scope of the analysis from asymmetrical faults to all failures that are capable of affecting more than one of the redundant trains of the electrical power supply system. This includes non-redundant components or systems like the grid connections, the generator or the generator bus duct, but also redundant components inside and outside of the safety systems that have caused impairments in more than one train during a failure event.

Since German operating experience with NPPs is limited to about 800 reactor years, it was decided to extend the scope of the analysis. Based upon an evaluation of the technical comparability of the plants, the accessibility of the necessary information and the amount of available data, it was decided to use the operating experience of the U.S. NPPs as it is provided through the Licensee Event Reports (LER) as additional information source. Although all these events have already been analysed in depth by the U.S. NRC, it was concluded that additional insights from the events could be gained by an analysis focused on possible effects on modern KWU type plants, which have a safety system that relies primarily on redundancy rather than diversity.

Table 2: Parameter combinations for asymmetric faults

No.	Type of failure	Location of failure	Plant condition	Neutral point treatment
1	Single phase	Main grid breaker	Power operation (full load)	Ungrounded /open
2	Single phase	Main grid breaker	Power operation (full load)	Solidly-grounded
3	Dual phase	Main grid breaker	Power operation (full load)	Ungrounded /open
4	Dual phase	Main grid breaker	Power operation (full load)	Solidly-grounded
5	Single phase	Main grid breaker	Outage, low[†] onsite power consumption	Ungrounded /open
6	Single phase	Main grid breaker	Outage, low onsite power consumption	Solidly-grounded
7	Dual phase	Main grid breaker	Outage, low onsite power consumption	Ungrounded /open
8	Dual phase	Main grid breaker	Outage, low onsite power consumption	Solidly-grounded
9	Single phase	Auxiliary grid breaker	Outage, low onsite power consumption	Ungrounded /open
10	Single phase	Auxiliary grid breaker	Outage, high[‡] onsite power consumption	Ungrounded /open
11	Dual phase	Auxiliary grid breaker	Outage, low onsite power consumption	Ungrounded /open
12	Dual phase	Auxiliary grid breaker	Outage, high onsite power consumption	Ungrounded /open
13	Single phase	Grid connection (50 km distance)	Power operation (full load)	Ungrounded /open
14	Dual phase	Transmission grid	Power operation (full load)	Ungrounded /open
15	Single phase	Main grid breaker	Power operation (partial load)	Ungrounded /open

3.3. Operating experience analysis methodology

Effects with the potential to affect multiple redundant trains simultaneously are rare since extensive precautionary measures are taken to avoid such events. Therefore, a substantial amount of operating experience has to be analysed to identify some of these types of failures. To achieve this, all 3466 LERs with events in PWRs and BWRs from the beginning of the year 2000 to the end of 2009 were included into the scope of the analysis. To cope with this high number of events in a reasonable amount of time, a four stage process was developed to identify the relevant fault scenarios:

1. Initial screening of the events; based upon an event summary, all available events are screened to filter out all those events that are obviously not relevant for a further analysis.
2. Thorough analyses of the remaining events to further reduce the number of events; at this stage all information included in the LER is used for the assessment.
3. The remaining events are analysed and described in depth by taking into account all available information.
4. Based upon the results achieved in step 3, failure scenarios (see Section 3.1) are developed.

The first step of the process resulted in 250 potential events, which were reduced to 29 events in step two. They cover a wide range of effects like external impacts (severe weather or grid fluctuations),

---

[†] I.e. one train of the residual heat removal system is operating.
[‡] I.e. all trains of the residual heat removal system are operating.

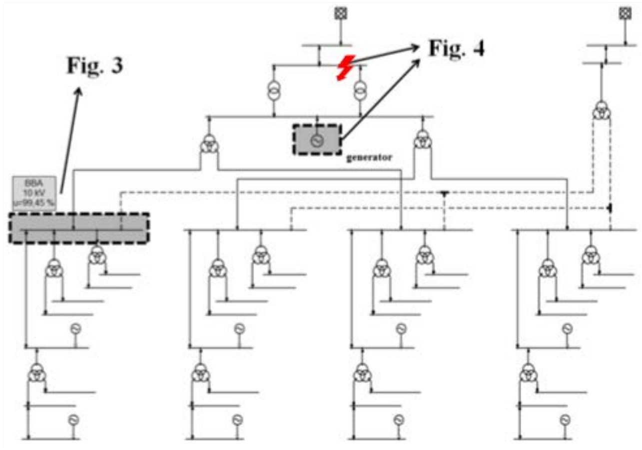
component failures inside the plant or in the associated switchyard, or events due to human error. Therefore, it may be expected that a comprehensive set of relevant failure scenarios will result from this effort. In addition to the asymmetric faults, the following phenomena from operating experience have been recognised as potentially relevant for an analysis:

- Static (long lasting) deviations from the specified voltage and frequency in the transmission grid
- Voltage fluctuations due to the extensive use of STATCOMs
- Failures in the voltage controller of the main generator
- Voltage transients due to component failures in the onsite power supply system

4. DEVELOPMENT OF A DETAILED DYNAMIC MODEL

A generic model of the auxiliary power system of modern German KWU type NPPs has been developed using the software NEPLAN [6]. Using this model, different calculations and analyses can be performed, such as load flow calculations, short circuit calculations, harmonic analysis, and dynamic simulations.

Figure 2: Generic model of the auxiliary power system of a German NPP. On each bus bar, several individual electrical consumers are modelled (see Figure 3)



The model currently consists of 733 elements (including 114 asynchronous machines as consumers) so far (see Figures 2 and 3) and is continuously being further developed. It is suitable for estimating the impact of different scenarios on the NPP's safety system. As an example, Figure 4 shows total power and frequency at the generator terminal after a single-phase interruption at the connection to the grid (shown as an arrow in Fig 3). Currently it is used for the detailed investigation of the scenarios mentioned above to examine the failure modes and effects.

Figure 3: One of the four main 10 kV bus bars with electrical consumers

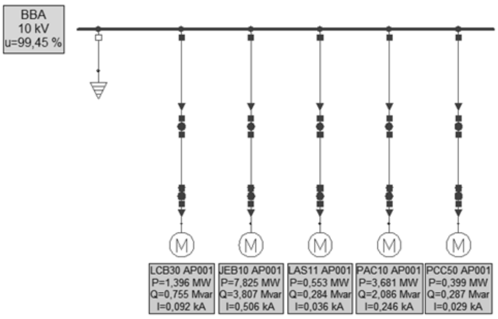
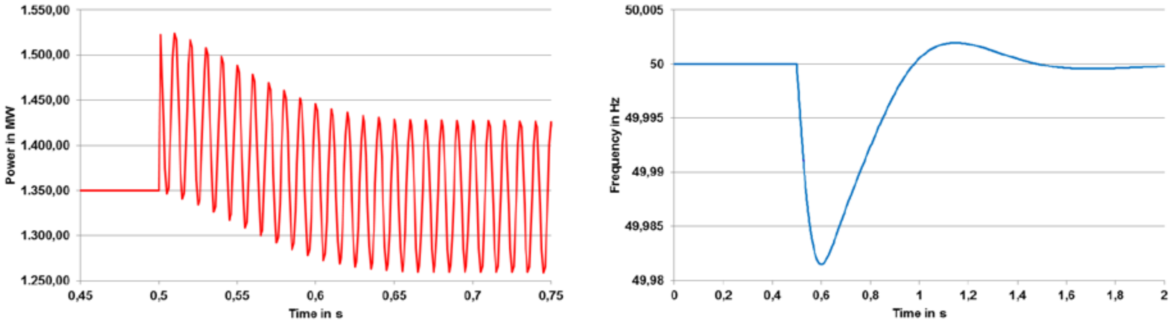


Figure 4: Total power and frequency at the generator terminal for a single-phase interruption of the connection to the grid (see Figure 2) occurring at t = 0.5 s



5. PROBABILISTIC MODEL

First analyses have shown that the appropriate modelling of realistic single phase failure scenarios and other scenarios simultaneously impairing multiple trains of the electrical power supply system in a PSA requires extensive augmentation and modification of present PSA models. This comprises modelling the complex impacts of such phenomena on the electrical equipment, including parts of the electrical power supply system not important to safety, in the PSA model and adding additional failure modes of electrical components already modelled. To efficiently and systematically integrate such modifications into existing PSA models, GRS has developed and is continuously improving the software tool “pyRiskRobot” for modifying complex fault tree topologies in an automated and traceable manner [7]. This tool will facilitate modifying and enhancing the PSA model.

In order to estimate the frequency of relevant initiating events emerging from an asymmetry in the electrical power supply, fault trees are used. The unavailability of relevant safety functions as a result of component failures under such conditions will also be modelled with fault trees. Two examples of fault tree modelling are shown in the following.

Firstly, the initiating event frequency for the initiating event “Reactor shutdown due to unavailability of 2 or more reactor coolant pumps after single phase failure in the auxiliary power supply” is computed with the fault tree shown in Figure 5.

Secondly, the fault tree for modelling the unavailability after a phase failure in the auxiliary power supply of the startup and shutdown pump 1 as a representative for standby components is shown in Figure 6. The startup/shutdown pumps are used for feedwater supply to the steam generators during the startup and shutdown phase. The availability of these pumps is essential for the availability of the safety function steam generator feed. Before modifying the model to include phase failure scenarios, the fault tree shown in Figure 6 contained the single startup failure P-SSP1-DNS and the common cause failure CCF-SSP12-DNS of the startup and shutdown pumps. Newly added was the basic event P-SSP1-DNSPF with the conditional failure probability of startup/shutdown pump 1 in case of a single phase failure in the auxiliary power supply. The house event H-PF allows for switching on and off the open phase condition.

In order to complete the PSA model modifications, the frequencies of all relevant initiating events after phase failures and the conditional unavailabilities of all relevant safety functions will be modelled by fault trees similar to those shown in the two examples. Furthermore, the consequential accident sequences will be identified and implemented in the PSA model.

Figure 5: Fault tree for computing the initiating event frequency of “Reactor shutdown due to unavailability of 2 or more reactor coolant pumps after single phase failure in the auxiliary power supply”

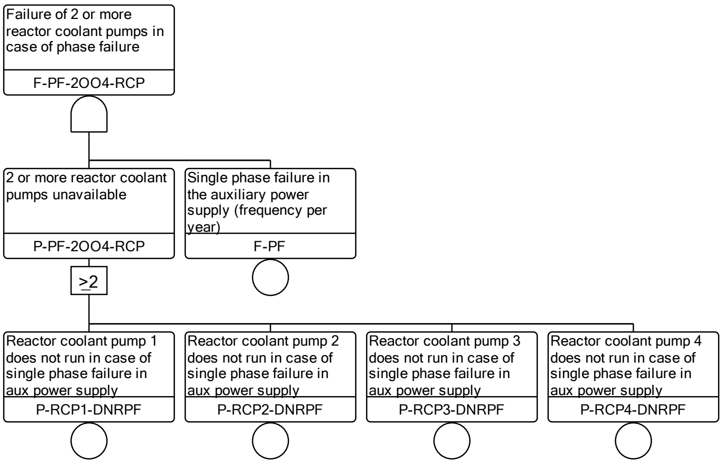
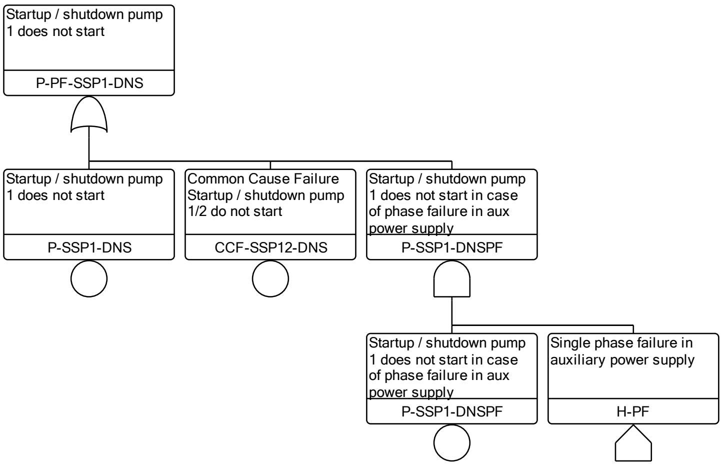


Figure 6: Fault tree for computing the unavailability of startup/shutdown pump 1



6. QUANTIFICATION

To quantify the model, the frequencies of the new initiating events and additional reliability parameters need to be estimated including e.g. failure probabilities and failure rates for electrical equipment that is or has been exposed to asymmetries in the electrical power supply.

As a first step, the rates of the initiating events “single-phase failures in the active grid connection” and “dual-phase failures in the active grid connection” and the unavailabilities of the non-active grid connection due to single-phase failures and dual-phase failures have been assessed utilizing the entire international operating experience of NPP (see Chapter 1 and [8]) The observation time is 16537 reactor years. Asymmetries lasting very short times (i.e. shorter than 500 ms), e.g. due to a lightning strike or when the automatic detection and clearance of a fault have succeeded, have not been included. Statistical tests show that international operating experience may be treated as homogeneous. Nine events occurred in the active grid (see table 1[§]). Three of these affected two units of multi-unit plants. In two cases, two phases were affected. Three events occurring in the non-active grid affected single units and lasted 21, 26, and 1 day, respectively. In all these three events only a single phase was affected.

[§] The duration of the asymmetry in the Koeberg NPP was estimated to be less than 500 ms. Therefore this event has not been included.

To assess the uncertainty of the estimates of failure rates and unavailabilities, Bayesian statistical methods were applied. To consider the features that multiple units of a plant may be affected by a failure and that a broad distribution of unavailability times of the non-active grid has been observed, two and three stage stochastic models were applied. The failures of the active grid were modelled with a discrete compound Poisson distribution with a categorical distribution as secondary distribution, which quantifies the probabilities μ_i that i units are affected. The failures of the passive grid were modelled as compound Poisson process with a categorical distribution as secondary distribution, which here also quantifies the probabilities μ_i that i units are affected, and with an exponential distribution as jump size distribution.

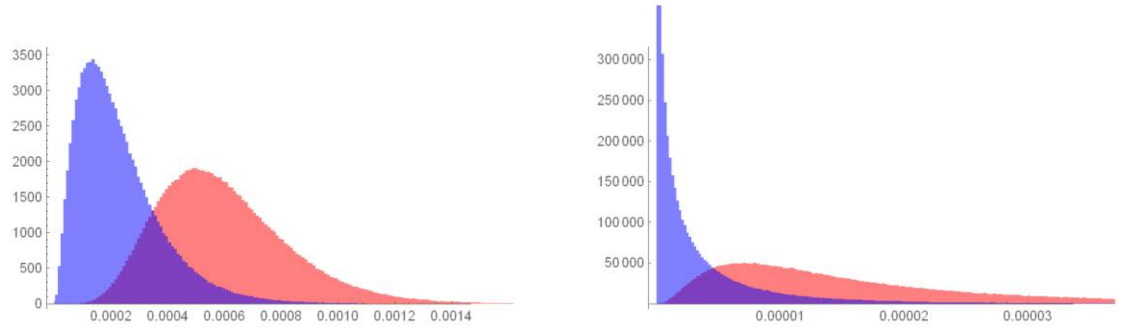
Since no events were observed for two-phase failures in the passive grid, the distribution of parameters of the jump size distribution for the one-phase case was used. The rationale of this is as follows. If two-phase failures had been present in the events observed, they would most likely have been discovered in the same way and the same time frame as in the actual observed events with one-phase failures.

For the model parameters, non-informative prior distributions according to Jeffreys have been chosen. The a posteriori distributions of the model parameters can be calculated analytically as Gamma and Dirichlet distributions while the desired uncertainty distributions of the unavailabilities and rates were estimated with Monte Carlo methods (sample size 10^6).

One should bear in mind that the operating experience described above may be incomplete. While significant asymmetries of the active grid – even if they may not be licensee reportable events by themselves – may be assumed to lead at the very most to failures of equipment important to safety and/or plant transients that are reportable. This is not the case for asymmetries of the non-active grid. Since in this case no immediate impact on plant equipment can occur only major unavailabilities of the non-active grid may be reportable. The reportability of such unavailabilities is typically limited to long time unavailabilities (e.g. larger than 72 h) and specific plant states (e.g. power operation). To consider this, firstly the observation time for the calculations of the unavailabilities of the non-active grid was limited to the time of power operation, which was conservatively estimated as product of the observation time of all operating reactors and the mean unit capability factor [8], resulting in an effective observation time of 12899 reactor years. Secondly, it was investigated how the estimations of the unavailabilities of the non-active grid depend on possible additional (unreported) events with short unavailability times. There is no significant dependence. Hence it was concluded that the uncertainty associated with unreported events with short unavailabilities may be disregarded.

The probability density functions of the uncertainty distributions are depicted in Figure 3 and their main characteristics are shown in Table 3.

Figure 6: Uncertainty distributions of the rates of one-phase (left, blue) and two-phase (left, red) failures of the active grid and of the unavailability of the non-active grid due to one-phase (right, blue) and two-phase (right, red) failures



To quantify the model, the conditional failure probabilities of components exposed to asymmetries in the electrical power supply also need to be estimated. Preliminary analyses of the operating experience have shown that such failures usually have the character of common cause failures. With high probability, identical and similarly loaded components fail together. Further research will be devoted to the development of methods to model and quantify this.

Table 3: Characteristics of the uncertainty distributions of the rates of one- and two-phase failures of the active grid and of the unavailability of the non-active grid due to one- and two-phase failures

	Rate of one-phase failures of the active grid in 1/a	Rate of two-phase failures of the active grid in 1/a	Unavailability of the non-active grid due to one-phase failures	Unavailability of the non-active grid due to two-phase failures
5% Quantile	2.79 E-04	4.98 E-05	3.40 E-06	1.07 E-08
Median	5.64 E-04	1.94 E-04	1.35 E-05	1.28 E-06
Mean	5.95 E-04	2.27 E-04	2.01 E-05	3.84 E-06
95% Quantile	1.02 E-03	5.16 E-04	5.68 E-05	1.54 E-05
99% Quantile	1.27 E-03	7.18 E-04	1.12 E-04	3.60 E-05

The rate of one- and two-phase failures in the active grid connection is comparable to the rate of small loss of coolant accidents (LOCAs).

7. CONCLUSION

Faults affecting multiple redundant trains of the electrical power supply system of NPPs – including but not limited to open phase conditions – may pose a significant threat to the safety of NPPs. Such failures have generally not been appropriately considered in PSAs. An on-going project of GRS to research this subject comprises the systematic analysis of national and international operating experience, the development of a detailed dynamic model of the electrical power supply system and the extension and modifications of an existing PSA model and the quantification of the enhanced model. The advancements made so far suggest that substantial new insights will be gained in the frame of this project. First results show that the rates of single- and dual-phase failures in the active grid connection are comparable to the rate of small LOCAs. The modelling and quantification of the reliability of components exposed to asymmetries, however, still poses a significant challenge.

Acknowledgements

This research has been funded by the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU).

References

[1] B. Brück, et. al. "*Implications of Open Phase Conditions in the Electrical Grid Connections for the Safety System of NPPs*", EUROSAFE, Munich, Germany, (2016).

[2] O. Mildenberger. "*Vertiefte Untersuchungen von Betriebserfahrungen aus Kernreaktoren*", GRS-458 (in German, with an English abstract), Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Cologne, Germany, (2017).

[3] International Atomic Energy Agency (IAEA). "*Design of Electrical Power Systems for Nuclear Power Plants*", IAEA Safety Standards Series No. SSG-34, Vienna, Austria, (2016).

[4] U.S. Nuclear Regulatory Commission (NRC). "*Significant loss of safety-related electrical power at Forsmark Unit 1 in Sweden, Information*", Notice 2006-18, Supplement 1, (2007). https://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2006/in200618sup1.pdf

[5] Reaktor-Sicherheitskommission (RSK), "*Scheibenübergreifende Unverfügbarkeiten aufgrund elektrischer Kopplungen zwischen redundanten Scheiben des Notstromsystems deutscher Kernkraftwerke*", RSK-Stellungnahme, 472. RSK-Sitzung, (January 14, 2015), (in German), http://www.rskonline.de/sites/default/files/reports/epanlagersk472hp.pdf.

[6] NEPLAN, NEPLAN AG, Küsnacht, Switzerland, http://www.neplan.ch/.

[7] N. Berner and J. Herb. "*Generic framework for the automated integration of impacts from hazards in PSA models*", Risk, Reliability and Safety: Innovation Theory and Practice, Walls, Revie and Bedford (Eds.), pp. 2645-2649, (2016).

[8] International Atomic Energy Agency (IAEA). "*Nuclear Power Reactors in the World,*" Reference Data Series No. 2, Edition 2016, Vienna, Austria, (2016).