EXPENDING THE SCOPE OF ICDE: SYSTEMATIC COLLECTION OF OPERATING EXPERIENCE WITH CROSS COMPONENT GROUP CCFS

Benjamin Brück[1], Dr. Albert Kreuser[1], Dr. Jan Stiller[1], Moritz Leberecht[1]

[1]: Gesellschaft für Anlagen- und Reaktorsicherheit (gGRS mbH), Schwertnergasse 1, 50667 Köln, Germany
benjamin.brueck@grs.de

Multiple simultaneous unavailabilities of components within the safety system of nuclear power plants (NPP) are generally not covered by the design-basis of NPPs and may therefore potentially lead to beyond design-basis accidents. Since these unavailabilities are most likely caused by common cause failures (CCFs), comprehensive precautionary measures against CCFs are essential for nuclear safety. The analysis of the operating experience of NNPs as method to get qualitative and quantitative insights regarding CCF mechanisms, consequences and probabilities is well established for decades. Currently, "common cause component groups"(CCCG) are used as basic element for qualitative and quantitative CCF analysis. Such CCCGs consist of multiple redundant components with a similar design which perform the same task in the plant's safety system. Up to now, CCF data collection is mostly focused on individual CCCGs so events which may impair multiple component groups at once are beyond the scope of data collection, modelling and PSA analysis. This leads to a systematic, yet quantitative unknown underestimation of the calculated core damage frequency. The aim of this paper is to promote the concept of CCFs which affect multiple CCCGs at once – so called "Cross Component Group CCFs" (X-CCFs) and how to perform data collection on such failures.

I. INTRODUCTION

Due to the high degree of redundancy in the safety system of nuclear power plants (NPP) multiple simultaneous failures of components are necessary to threaten the safety goals of NPPs. The most common cause of such multiple simultaneous failures in high redundancy systems are Common Cause Failures (CCFs). CFFs are failure events in which two or more component fault states exist simultaneously and are a direct result of a shared cause. Depending on the design of the NPP's safety system and the used PSA-methodology CCFs may contribute up to 95 % (Ref. 1) to the total probability for core damage tates. It is therefore a matter of importance to ensure that a comprehensive understanding of all phenomena which may lead to CCFs of components which are used in the safety system of NPPs is gained.

CCF analysis and modelling in PSA is based on common cause component groups (CCCG). In practice, a CCCG is defined as a set of identical or similar components which perform the same function in the NPP's safety system and that can be affected by CCF failure mechanisms. Right now the CCCG are regarded as independent from each other with individual CCF probabilities. In this modeling approach, each CCF affects only one individual CCCG. Thorough analysis of operational experience from NPPs suggests that the assumption that the CCCGs are actually independent from each other is not appropriate for all component types or failure mechanisms. In fact, there are numerous obvious or hidden dependencies between such two groups like common maintenance teams and procedures, piece parts which are used in both groups, shared cooling water, superordinate I&C or internal and external factors which may affect both groups simultaneously. Such interdependencies as described above potentially affect all component types. Even CCFs which affect CCCGs of different component types are possible. These "Cross Component Group CCF" (X-CCF) constitute an additional risk for component failures which are not thoroughly addressed by current PSA modelling.

Some of these interdependencies are well known, modelled and quantified in PSA (e.g. fire (Ref. 2) or internal flooding (Ref. 3)) others are basically known but not quantified or stringently modeled (e.g. dependencies due to common piece parts or procedures) and finally a third group of dependencies is completely unknown or unrecognized until the moment of their appearance. An example for this type of interdependencies emerged at two events in the NPP Byron, Unit 2 on January 30th 2012 and in the NPP Forsmark, Unit 3 on May 30th 2013 where an open phase condition (OPC) in the active grid connection of the plants caused an asymmetric voltage inside the whole onsite power system. This led to the simultaneous unviability of

numerous electrical drives across several component groups. This type of failure was – although theoretically known – not assessed or modeled in any way.

The objective of this paper is to show the necessity to include the cross component aspect into the scope of CCF research by presenting several real word examples where Cross Component CCFs have been observed in NPP. By doing this, it will focus on the operating experience and how to analyze it and not on the PSA-modelling aspects. It will be discussed what information is necessary to identify, analyze and quantify X-CCFs and how the ICDE database can be used in this process.

For the purpose of this paper a (potential) X-CCF is defined as a simultaneous (potential) impairment state of multiple components from different CCCGs due to the same failure mechanism.

II. CURRENT CCCG-MODELLING AND PROBLEM DEFINITION

According to Ref. 4 the first step in each CCF analysis is the qualitative screening of the NPPs safety system to identify CCF vulnerabilities and to define the CCCGs. This process is the foundation of any further PSA-modelling. Without a comprehensive and complete modelling of the CCCGs and the collection of the associated reliability data no for meaningful PSA results can be calculated.

As described in Ref. 5 and Ref. 6 the compilation of CCCGs is always a compromise between the requirement to cover all possible coupling mechanisms on the one hand and the necessity to create manageable, task related group sizes on the other hand. The actual outcome of the compilation process differs from country to country; in some cases, all components of a certain component type in one system (e.g. all motor operated valves (MOVs) in the emergency core cooling system) are grouped in one CCCG while the MOVs in the auxiliary feedwater system form another one, in other country the focus is on the task of the component so for each position within the redundant trains of the plants safety system a separate CCCG is created. The first method creates fewer but larger CCCG, the second method creates more, but smaller CCCGs. When taking the list of possible coupling mechanisms from Ref. 4:

- Design
- Hardware
- Function
- Installation, maintenance or operations staff
- Procedures
- System/Component Interface
- Location
- Environment

it becomes quite clear, that both approaches do not ensure that the defined component groups are independent from each other in a way that no CCFs-mechanisms can be assumed which affect more than one CCCG simultaneously. Taking the above mentioned MOVs as example, even for the system-wide CCCGs failure mechanisms originating from system/component interfaces or from installation or maintenance errors may lead to X-CCFs e.g. when MOVs in different systems are affected simultaneously.

For each of the component types for which CCCGs are created, “component boundaries” have to be defined. These component boundaries define the interface of the component with the rest of the plant. Only failures inside the component boundaries are regarded as failures of the component. Taking centrifugal pumps as an example, the component boundary may include the pump itself, the motor, the motor-cooler, the pump specific switchyard equipment (circuit breaker), pump specific I&C and the corresponding cabling. It excludes the suction- and pressure-side valves, the superordinate I&C, cooling water supply and room cooling. Refining the component boundaries (e.g. separating the circuit breaker from the rest of the component) may contribute to the prevention of unrecognized and unanalyzed failure mechanisms which may affect multiple CCCGs. In the aforementioned example, comparable circuit breakers from different pumps would be collected in a separate CCCG with corresponding CCF-probabilities, so CCF failure mechanisms which may affect all pumps with these types of breakers can be modeled correctly. This refinement of component boundaries may improve CCCG-modelling, but will not solve the problem of X-CCFs entirely. First of all, the refinement is limited due to practical reasons; it is not feasible to identify all piece parts or auxiliary agents (e.g. lubricants) which are used in more than one CCCG and to define additional CCCGs for them. Furthermore, unknown “new” failure mechanisms like the aforementioned OPC couldn’t be modeled with

refined CCCG either. Based upon these generic considerations it is concluded that the existence of X-CCFs has to be assumed and therefore further analyzed.

III. EXAMPLES FROM THE OPERATING EXPIERENCE

In section I of this paper three groups of possible interdependencies between CCCGs were identified, which can be distinguished by the degree of uncertainty which exists with respect to the failure mechanisms, failures consequences and effective coupling factors between the involved CCCGs. These three types can be defined as follows:

- Type 1: Well-known, modelled and quantified phenomena like fire or flooding. These types of failure mechanisms which may impair multiple CCCGs simultaneously will not be discussed further in this paper.
- Type 2: Phenomenological known interdependencies such as common piece parts, auxiliary agents or procedures, which are not stringently modelled or quantified. Deepened analysis of the operating experience with NPP can help to complete the list of failure mechanism and in the long run to quantify the probability that a CCCG is affected by a specific failure mechanism.
- Type 3: Effects which are completely unknown before the moment of their first appearance. After this moment, they belong to type 2, but even before that moment operational experience can be used to identify interdependencies which serve as "propagation path" for X-CCFs. This information can be used to reassess and improve the diversity within the NPP's safety system.

In the following sections some examples for Type 2 and Type 3 interdependencies which caused (potential) X-CCFs in real world events in the German and international operation experience are given:

III.A. Example 1: Common Piece Parts and maintenance procedures in different emergency diesel generator CCCGs

III.A.1. System description

The emergency power supply system of German PWR consists of four trains with one ~5000 kW diesel generator ("D1 diesel") in each train. With these emergency diesel generators (EDGs) all components and systems relevant for the safety of the NPP can be supplied with electrical power, furthermore some consumers like the heating of the pressurizer which are not necessary for incident handling, but that add additional safety margins. In addition to the large diesel generator there is a smaller diesel ("D2 diesel") with ~800 kW in each train which serves both as drive for the emergency feedwater pumps and as generator to supply some essential loads like a basic residual heat removal system. These smaller diesels are bunkered to maintain their safety function also in case of events like explosions or airplane crashes. The capacity of these diesel generators is not sufficient to supply all safety relevant loads, e.g. they are not capable to supply all consumers which are required to handle all kinds of LOCA-events. Due to the differences in capacity, construction and function both groups of diesels are handled separately in PSA modelling so there is a separate CCCG for each kind of diesel generator. In the following section, some events from the German operating experience are presented which suggest that this modelling is questionable.

III.A.2. Event No. 1: Potential X-CCF due to common piece parts (Ref. 7)

The plant was in full power operation. During recurring testing, one of the D2 diesel failed to achieve the test objectives since it did not reach its rated power-output. Subsequent inspection of the diesel revealed that both turbochargers of the diesel were severely damaged by foreign objects which were introduced into the turbochargers. It was determined that these foreign objects originated from extension-joints in the air-intake piping upstream of the turbochargers. The objectives parted from the expansion joints due to inadequate assembly works at these joints. Further inspections showed that at all D2 diesels and all D1 diesels the expansion joints were also inadequately assembled.

The quantification of the risk that also at other diesel generators objects from the expansion joints get loose and damage the turbochargers is difficult since it is apparent that the failure mechanism described above does not progress by stand-by-time but by run-time. Typical for stand-by components in the safety system of a NPP the EDGs are normally operated only for testing purposes. Hence, it takes several years for them to collect their required mission-run-time during testing. From an engineering point of view it is not possible to predict how long the other diesel generators would have been able to run before they would have also failed due to turbocharger damages. According to the coding scheme which is used by ICDE (Ref. 8) to quantify the extent of the impairment of a component (**C**omplete Failure, **D**egraded, **I**ncipient, **W**orking) the directly affected

EDG can be assessed as "C" (complete failure), the 7 other ones can be assessed as "I" (Incipient). When integrating the observed degradations into an "impairment vector" this would be [*CIII / IIII*] for the two CCCGs.

Summarizing it can be stated, that a single failure mechanism (inadequate assembly work at expansion joints) affected two EDG CCCGs simultaneously which is in accordance with the definition of a X-CCF irrespective of the actual quantitative assessment of the component impairment. The coupling mechanism in this example is a common piece part and associated with this common piece part common assembly procedures in both CCCGs. The expansion joints used in in the two CCCGs were not identical (the ones used for the D1 diesel have a larger diameter than the ones used for the D2 diesel) but sufficiently similar that the arisen failure mechanism affected both CCCGs.

This event constitutes an example of an interdependency of type 2 as defined above. The fact that common piece parts which are used in different CCCGs have the potential to fail more or less simultaneously is basically known but not stringently modelled right now. It is impractical to dissolve the interdependency by refining the component boundaries since this would increase the number of CCCGs and component types in a way that is not manageable. The most effective way to include events like the one described above into the scope of CCF-modeling would be the introduction of yet to be defined coupling factors between the CCCGs with comparable components.

III.A.3. Event No. 2: Potential X-CCF due to misleading maintenance/testing instructions (Ref. 9)

The plant was in refueling-outage. During recurring testing the automatic initiation of the EDG startup sequence was disabled and not returned into nominal condition after completion of the testing. This was done for all D1 diesels and all D2 diesels, so in case of a LOOP event no diesel would have started automatically on RPS/ESFAS command. The EDGs themselves were not impaired and available for a manual start-up all the time. Subsequent analysis showed that the unavailability of the EDGs persisted for about 15 hours. During this time period, there was no demand for any EDG.

In the moment when the event was discovered, all eight EDGs were completely unavailable. In the given situation the impairment vector of the two CCCGs was [*CCCC / CCCC*]. For applicable quantifying of the impairment of the affected components, also the plant state has to be taken into account. The recurring testing which led to the event is done only during outage of the plant. This specific erroneous configuration of the EDG actuation should be discovered during the final tests before start-up of the NPP at the latest. Nevertheless, it cannot be assumed, that this is the case for all types of possible errors which may occur during maintenance activities which affect both EDG CCCGs.

For this event, the coupling mechanism between the two CCCGs is a misleading procedure for the recurring testing of the EDGs. From modelling perspective it is questionable whether the event happened outside or inside the component boundaries of the diesel – in the following examples it can be seen that it is a quite common phenomena for X-CCFs that it is difficult to assign the failure to a specific component or a specific group of components. Instead these failures are often located at the "boundary" of the components.

According to the definitions given above, this event can also be assessed as Type 2 interdependency. It is well known that a proper function of the superordinate RPS/ESFAS I&C is necessary for the function of the EDGs, but it is not clear how to include this aspect into the modelling. This can be achieved via an appropriate modelling of the superordinate I&C or by the introduction of coupling factors which model the behavior of this I&C.

III.B. Example 2: Unmodeled meshing inside the emergency core cooling and residual heat removal system (Ref. 10)

The emergency core cooling and residual heat removal system in German PWRs consist of four trains. Each train has one high pressure safety injection pump (HPSI) and one low pressure safety injection pump (LPSI) and several isolation and control valves. Both pumps in each train draw their water from a single refueling water storage tank.

In the German operating experience two events are recorded where the liquid content of several of the refueling water storage tanks was outside of the specification. In one event the boron concentration was below the specified value in three of the four tanks. The reason for this deviation was a misalignment of hand-valves which caused the tanks to be filled with pure demineralized water instead demineralized water with the appropriate boron concentration. In another event the liquid level in all four tanks was below the specification. This was due to misinterpreted signaling about the water level. Both events have been assessed as INES 2 events.

It is obvious that both failure mechanisms impacted outside the component boundary of any active component (pumps and valves) in the emergency core cooling and residual heat removal system. Nevertheless, both failure mechanisms had the potential to render the safety function of both the HPSI and LPSI pumps – which is the injection of a sufficient amount of water with a sufficient boron concentration into the primary circuit – useless. In recent PSA for German NPPs the state (level, boron concentration etc.) of the refueling water tanks is not modeled at all. Furthermore, no reliability data for the state of these tanks is available. Even though this approach is consistent with the assumptions made in Ref. 5 that PSA results are dominated by the active components and therefore the modelling of many passive components can be omitted, the event demonstrates that there is an unmodeled interdependency between several active CCCGs in the emergency core cooling and residual heat removal system. In this case it is questionable, whether the event can be interpreted as X-CCF since it is difficult to figure out which component groups are actually affected.

This event constitutes another example for a Type 2 interdependency. The fact that both the HPSI and the LPSI relay on the availability of the water inside the same refueling water storage tank is of course well known, but the corresponding modelling is not appropriate. Since it is not possible to assign the failure mechanisms to a certain component this event illustrates – in contrast to the ones above – that the introduction of coupling factors between CCCGs is not always an appropriate choice. Events like this are most likely better handled by an improved modelling in PSA which covers also the role of the refueling water storage tanks.

III.C. Example 3: ASYMMETRIC FAULTS IN THE GRID CONNECTION OF NPPS

The two events described below are probably the most interesting ones when dealing with X-CCFs. In both events a single failure outside the safety system of the NPP rendered several CCCGs even of different component types inside the safety systems completely useless due to a common failure mechanism which affected all these CCCGs simultaneously. The cause of these failures was an asymmetry in the NPP's onsite power system. As an introduction, some background information about such electrical asymmetries is given; after this the two events are described.

III.C.1. Technical Background

Almost all induction motors which are used as drive for pumps, valves or fans in the safety system of NPPs use three-phase alternating current as power source. The most important indicators for the quality of a three-phase alternating current are voltage amplitude, frequency and symmetry. A three-phase system is defined as "symmetric", when all three line-to-line voltages are equal and the distance between the three phases is about 120°. In Fig. 1 an example of a symmetric 50 Hz three-phase system with the three line-to-line (Lx-Ly) and the three line-to-neutral (Lx-N) voltages is given.

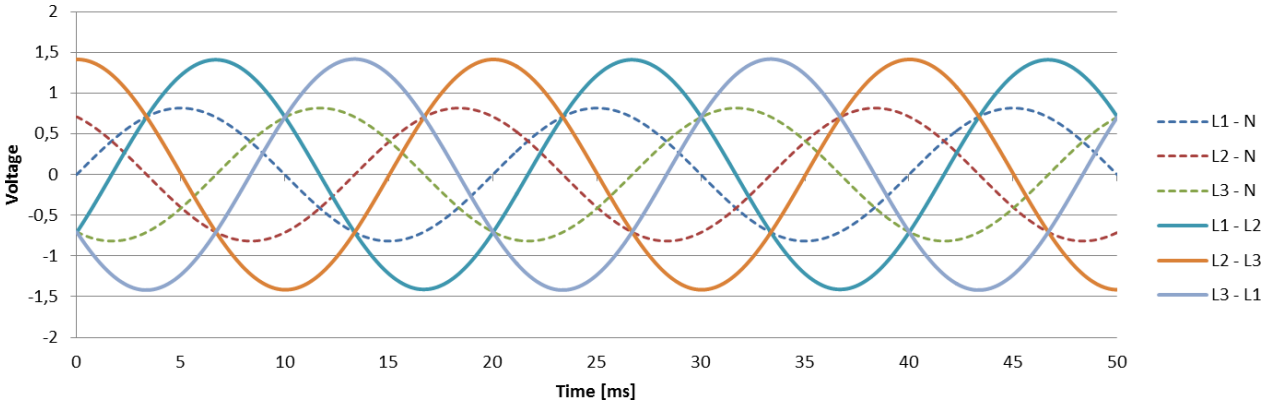

Fig. 1: Symmetrical three-phase system

In fact, electrical drives rely on certain minimum requirements for voltage amplitude, frequency as well as symmetry. While the effects of deviations from the specified voltage amplitude and frequencies are well known and well-monitored by the safety system of NPPs, the symmetry of the electrical power supply was outside of the scope of NPP safety research. In Fig. 2 an example of an asymmetrical voltage is given where L1-N drops to 50 % of the original value. Asymmetries may arise both due to deviations from the specified values of the line-to-neutral voltage amplitudes as well as from deviations of the phase sequence.

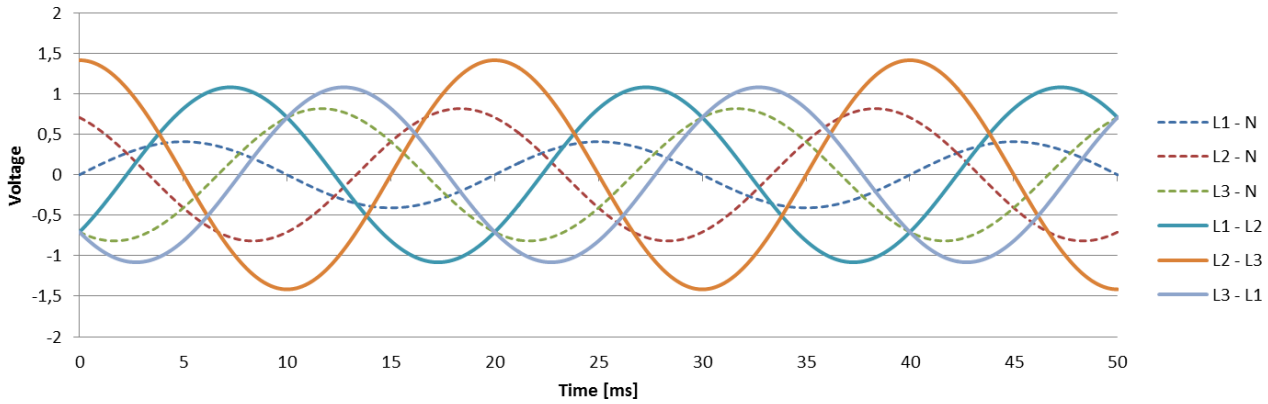

Fig. 2: Asymmetrical three-phase system

A detailed explanation of the effects which are caused by an asymmetrical voltage in an induction motor is not the topic of this paper, but summarizing, it can be stated that the current intake of the motor will rise while the torque will drop. The increased current intake may trigger overprotection devices or may even destroy the motor due to overheating. Even when just overcurrent-protection devices are triggered, the affected components have to be considered as unavailable for a certain amount of time since resetting the overcurrent protection devices in general requires manual actions in the switchyard building.

The reason why asymmetries in the power supply system are potentially a great threat for the safety of NPPs is due to the fact that during normal operation there is no stringent separation between the electrical redundancies. In Fig. 3 a schematic layout of a typical NPPs power system is given. As long as the plant is not in LOOP conditions all busbars including the safety busbars are connected either via the generator busbar or the high voltage side of the standby transformer.

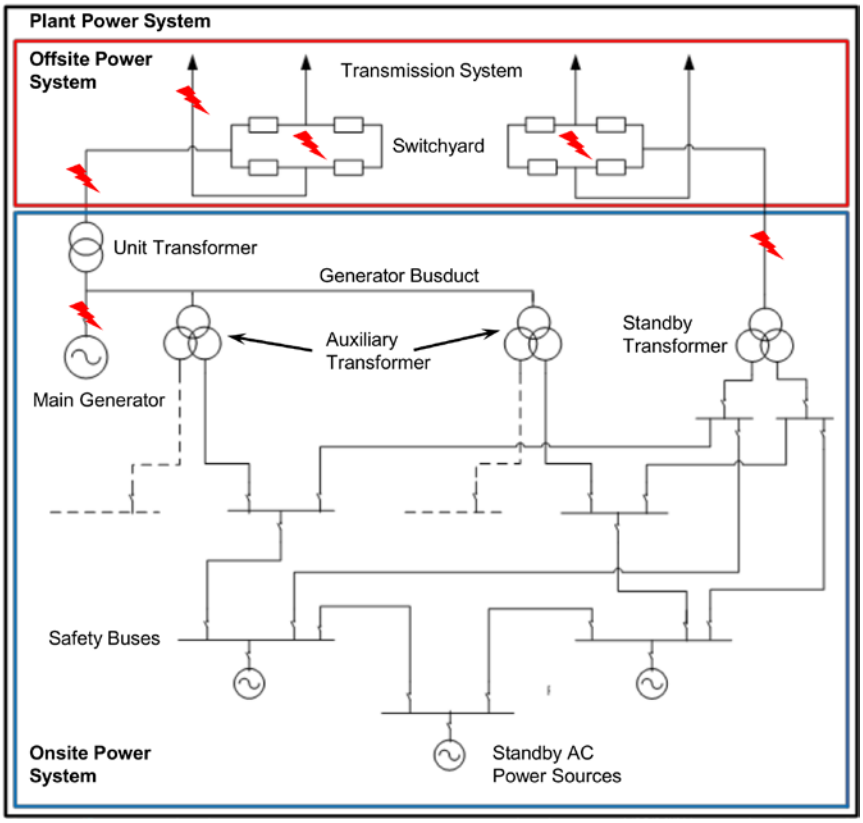

Fig. 3: Schematic layout of a NPP power system (Source: IAEA, modified)

Given that the safety buses are not supplied by the EDGs, all failures "above" the connection between the redundant busbars (examples for such failure positions are marked with a ↯ in Fig. 3 will affect all redundant busbars simultaneously. Even though the design of the onsite and offsite power systems may differ in detail from plant to plant, the connection between the electric busbars is a common characteristic of almost all NPPs.

The most common reason for persistent asymmetries are "open phase conditions" in the grid connection which is actually used to supply the plants onsite power system. The essential characteristic of an OPC is that one or two of the three phases is interrupted without any short circuit or ground fault so that there is no current flow in the affected phase. Such OPCs may be caused by failures of breakers which do not open or close in all three phases or by mechanical failures of conductors, busbars, isolators or other supporting structures.

III.C.2. Asymmetric fault in NPP Byron due to collapsed isolator (Ref. 11)

On January 30th 2012 Unit 2 of the Byron NPP was in full power operation, when a porcelain isolator on the high voltage side of the auxiliary transformers in the switchyard of the plant collapsed and caused an OPC. Even though one phase on the high voltage side was complete lost, due to the electromagnetic coupling of the three phases inside the auxiliary transformer two of the three line-to-line voltages on the low voltage side (4.16 kV nominal) did not drop to zero but to values of about 60% of the nominal voltage amplitude. Due to different voting logics inside the onsite power voltage monitoring system RPS sensed some problem and initiated SCRAM but did not cut the plants safety buses from the offsite power supply to initiate EDG-operation.

Consequently all electrical consumers in the plant remained connected with the fault and were exposed to an asymmetric voltage. Two seconds after the collapse of the isolator a first pump (essential service water (ESW) pump 2A) tripped because of over-current. In the following seconds a large number of other components which rely on inductions motors as drives tripped or failed to start because of over-current protection. Among them were a motor-driven auxiliary feedwater (AFW) pump, a condensate pump, all reactor coolant pumps and also several fans. Attempts of the shift crew to start pumps manually failed due to over-current trips of the pumps. For some minutes the reason for the behavior of the components remained unclear, the shift crew opened connections to unit 1 to restore ESW supply. After about 8 minutes a report was received from the field that smoke arose from the auxiliary transformers. Based upon this report, the safety busses were manually disconnected from the auxiliary transformers and the EDGs started automatically as designed to supply the safety busses. By doing so, the failure was disconnected from the safety busbars. After the safety busses were supplied by the diesels the necessary components were started and plant conditions were normalized.

III.C.3. Asymmetric fault in NPP Forsmark event due to non-opening poles of the 400-kV grid breaker (Ref. 12)

On May 30th 2013 unit 3 of the Forsmark NPP was in refueling outage. During maintenance works at the main generator the plant's unit protection was erroneously triggered and initiated a separation of the unit from the main grid which was used to supply the plant's onsite power system. Upon the command to open, only two of the three breaker poles of the 400-kV-breaker on the high voltage side of the unit transformers actually opened. The third one remained in the closed position. Hence, the plant's onsite power system was supplied by only one phase and experienced a significant voltage asymmetry.

As well as in the Byron event the RPS/ESFAS was not able to interpret the situation correctly and did not initiate any automatic action so that the onsite power system remained connected with the faulty grid connection. Within the next minutes in total 146 induction motors failed, either due to over-current trips or in a few cases even because of thermal destruction. Among other effects, all trains of the residual heat removal system of the plant were unavailable for about 15 minutes.

By using the voltage instrumentation in the central control room the shift crew was able to identify the persisting asymmetry as cause of the component failures and decided to separate the safety busbars from the plants grid connection and by doing so to initiate a start-up of the EDGs which subsequently supplied the safety busbars. Afterwards the plant conditions were normalized with the safety system supplied by the diesel generators.

III.C.4. Generic safety assessment of asymmetric faults in the grid connection of NNPs

Even though the direct consequences of the two events for the safety of the NPPs seem to be rather limited at first glance (the situation was cleared after ~10 minutes) there is a significant potential thread for the safety of NPPs due to such events.

A single failure of a component outside the plant's safety system caused the simultaneous unavailability of various safety relevant components from many different CCCGs of the safety system crew. It must be assumed that without manual actions of the shift crew nuclear safety goals would have been at risk within a short time. Moreover, the RPS/ESFAS was not able to detect the faulty state of the power supply system automatically. In case of the Byron event it even wasn't discovered by manual reading of the voltage instrumentation but because of smoke arising from the auxiliary transformers.

Even though asymmetric conditions in three-phase alternating current power system are well studied and understood in electrical engineering departments, it was completely out of the scope of NPP safety research and analysis. It was assumed that the external power supply was either available or not available. In the first case it could supply the onsite power systems, in the second case redundant EDGs would ensure that all systems relevant for the safety of the NPP are supplied with electrical power. The option that a condition in the external grid could persist which does not allow the operation of the consumer but that is not identified as faulty by the RPS/ESFAS system was not taken into account.

These two events constitute examples of Type 3 interdependencies as defined above. The effect which led to the X-CCF was completely new with regard to NPP safety and PSA modelling for NPP. No refinement of component boundaries or integration of dependencies and/or CCCGs would have been able to cover this type of failure mechanism. The coupling mechanism which caused the multiple component impairments is the common power supply during normal plant operation which is contrary to the concept of redundancy separation. A separation of the redundant busbars also during normal operation would enhance the resilience of the plants safety system against all types of external electrical faults.

IV. ROLE OF THE ICDE PROJECT

The examples presented above show very clearly that X-CCF are not only a theoretical idea but a real world phenomena which has been repeatedly observed in the operating experience of NPPs. Nevertheless, such CCFs do not occur very often, which makes a comprehensive analysis and assessment based on the operating experience difficult. With more than 1,650 CCF Events, 8,600 CCCGs ("Observed Population Records", OPs) and 152,000 Group Years the ICDE database is probably the largest collection of CCF related operation experience with NPPs. Hence, the ICDE database should be the ideal basis for a comprehensive and systematic search for X-CCFs. Right now, the database structure (Ref. 8) consists of OPs and CCF events which are linked to certain OP, each individual OP may have been affected by several CCFs, but each CCF is linked to exactly one OP. The database entries include both text fields for verbal event description as well as pre-defined fields for the event coding (e.g. for the root cause, the coupling factor or the time factor of the CCF event). This concept should be maintained as given; therefore the integration of the X-CCFs should be done by an additional structure which complements the existing database structures.

It has to be noted that the systematic integration of X-CCFs in the scope of PSA research requires efforts in several fields and reaches far beyond the area of operating experience analysis which is the main focus of the ICDE project. Right now it is not known which modelling approaches will be used and which data and information is necessary to quantify the additional risk due to X-CCFs with these yet to be developed modelling approaches. It has always been the goal of the ICDE project to perform the CCF data collection in a way that all information which might be is necessary for a qualitative or quantitative analysis is included, regardless of the used CCF model for quantification (α-factor, basic parameter, coupling model…). As mentioned above it is not known by now what information is needed for future needs, the data collection should cover as much information as possible to ensure greatest possible flexibility for the subsequent use of the data.

Based upon the current structure a second type of CCF event – the X-CCF – has to be introduced into the database. There are two possible ways to constitute a X-CCF within the ICDE database: Either multiple existing CCFs event entries with each of them connected with an OP-record, can be linked or completely new CCF event entries can be created which refer directly to multiple OP records. Regardless which way is used, as much as possible from the present information structure of the CCF event entries should be used. This comprises the Failure Mode, Impairment Vector, Root Cause, Coupling Factor, Shared Cause Factor, Corrective Actions and Time Factor. Additionally, as most important information, a detailed description of the observed failure mechanisms with special focus on the coupling mechanism between the multiple affected CCCGs has to be included.

First of all, this structure defined above has to be described in detail in a special coding guide for X-CCFs. The systematic approach for X-CCF analysis developed in Ref. 13 can be used as basis for this work. After this coding guide has been approved by the ICDE steering group, to fill this additional structure with real data will be a long-term task for all parties involved with ICDE. The potentially interesting events from the membership-countries operating experience have to

be identified and described according to the criteria described above. This applies both for events from the past which can be re-analyzed from the X-CCF-perspective and for recent events. After some operating experience has been gathered, workshops may be useful to draw conclusions from the collected operating experience. These conclusions may comprise quantitative as well as qualitative insights; for example the events in the ICDE database can be used to identify improved testing or maintenance procedures which may reduce the risk for X-CCF.

In summary the large amount of international operating experience with NPPs which is gathered in the ICDE database can be used as a foundation for further X-CCF research.

V. CONCLUSIONS

Even though some research has been already done (e.g. Ref. 13 and Ref. 14), the research regarding CCFs which affect more than one CCCG is just right at the beginning. This refers to operating experience and failure mechanism analysis as well as PSA modelling and quantification. From the examples given above three simple conclusions can be drawn:

1. Failure mechanisms which may cause CCFs that affect multiple CCCGs – called "Cross Component Group CCFs" or X-CCFs – are a real world phenomena. Ignoring such types of CCFs results in a systematic underestimation of the risk due to CCF in PSA. The quantitative extend of this underestimation is yet to be determined (see e.g. Ref. 14).
2. There are different types of X-CCFs. Some originate from incomplete modelling of basically well-known effects and interdependencies (Type 2), while others originate from really new effects and failure mechanisms (Type 3). Not all failure mechanisms which may affect multiple CCCGs simultaneously should be regarded as X-CCFs since some interdependencies originate from incomplete PSA modelling or from an inadequate definition of component boundaries. Therefore, in some cases an improved modelling with more CCCGs or refined component boundaries may be more appropriate
3. While CCFs are less frequent than single failures, X-CCFs are less frequent than "normal" CCFs. Large amount of operating experience is necessary to identify relevant failure mechanisms or to make a quantitative risk assessment. Therefore, international collaboration is essential.
4. The analysis of the operating experience with regard to X-CCFs should not only focus on the quantification of such phenomena but also on the qualitative analysis with the objective to identify precautionary measures e.g. in the areas of recurring testing and maintenance.

ACKNOWLEDGMENTS

This work was funded by the Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety (BMUB). The project was supported by Federal Office for Radiation Protection (BfS).

REFERENCES

1. U. HAUPTMANN, A. KREUSER and J. PESCHKE, *Vorgehensweise bei der Behandlung von GVA*, p. 4, grm, Merkel, Eggenstein, Germany (1994)
2. VON LINDEN, M. RÖWEKAMP, M. TÜRSCHMANN und H. P. BERG "Methods for a fire PSA exemplarily applied to a German BWR-69 type nuclear power plant", Kerntechnik vol. 72, no3, pp. 139-144 (2007)
3. EPRI, Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment (2009)
4. A. MOSLEH, D. M. RASMUSON, F. M. MARSHALL, *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, Prepared for U.S. Nuclear Regulatory Commission (1998)
5. FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSEN FÜR KERNKRAFTWERKE, *Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke*, BfS-SCHR-37/05, Salzgitter (2005)
6. FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSEN FÜR KERNKRAFTWERKE, *Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke*, BfS-SCHR-38/05, Salzgitter (2005)
7. BUNDESMINISTERIUM FÜR UMWELT NATURSCHUTZ UND REAKTORSICHERHEIT, *Meldepflichtige Ereignisse in Anlagen zur Spaltung von Kernbrennstoffen in der Bundesrepublik Deutschland – Jahresbericht 1997* (1998)
8. NUCLEAR ENERGY AGENCY, *International Common Cause Failure Data Exchange (ICDE) General Coding Guidelines*, NEA/CSNI/R(2011)12 (2011)

9. BUNDESMINISTERIUM FÜR UMWELT NATURSCHUTZ UND REAKTORSICHERHEIT, *Meldepflichtige Ereignisse in Anlagen zur Spaltung von Kernbrennstoffen in der Bundesrepublik Deutschland – Jahresbericht 1987* (1988)
10. BUNDESMINISTERIUM FÜR UMWELT NATURSCHUTZ UND REAKTORSICHERHEIT, *Meldepflichtige Ereignisse in Anlagen zur Spaltung von Kernbrennstoffen in der Bundesrepublik Deutschland – Jahresbericht 2003* (2004)
11. U. S. NCR, Byron Unit 2 – NRC Special Inspection Team (SIT) Report 05000455/2012008 (2012)
12. NUCLEAR ENERGY AGENCY, *ROBELSYS Workshop Proceedings Paris, France, 1-4 April 2014*, pp. 41-42. NEA/CSNI/R(2015)4 (2015)
13. M. LEBERECHT, J. C. STILLER, A. WIELENBERG, G. GÄNßMANTEL and A. KREUSER, *Entwicklung fortschrittlicher Methoden zur Identifizierung von Gruppen von Komponenten mit GVA-Potenzial und zur Bewertung von teilweiser Diversität*, pp. 181-182, GRS - 328, Germany (2015).
14. C. STILLER, G. GÄNSSMANTEL, M. LEBERECHT, A. KREUSER, C. VERSTEGEN, "Common Cause Failures Exceeding CCF Groups," to appear in the *Proceedings of the 13th International Conference on Probabilistic Safety Assessment and Management*, Seoul, Korea, October 2-7 (2016).