Recent Insights from the International Common Cause Failure Data Exchange (ICDE) Project

Benjamin Brück[a], Gunnar Johanson[b] , Michelle Gonzalez[c], Jan Stiller[a]
[a] Gesellschaft für Anlagen- und
Reaktorsicherheit(GRS) gGmbH, Cologne, GERMANY
[b] ÅF Industry, Stockholm, SWEDEN
[c] United States Nuclear Regulatory Commission, Washington, DC, United States

Abstract: CCF events can significantly impact the availability of safety systems of nuclear power plants. For this reason, the ICDE Project was initiated by several countries in 1994. Since 1997 it has been operated within the OECD NEA framework and the project has successfully operated over six consecutive terms (the current term being 2015-2017). The ICDE Project allows multiple countries to collaborate and exchange common-cause failure (CCF) data to enhance the quality of risk analyses, which include CCF modelling. Because CCF events are typically rare, most countries do not experience enough CCF events to perform meaningful analyses. Data combined from several countries, however, have yielded sufficient data for more rigorous analyses.

The ICDE project has meanwhile published eleven reports on collection and analysis of CCF events of specific component types (centrifugal pumps, emergency diesel generators, motor operated valves, safety and relief valves, check valves, circuit breakers, level measurement, control rod drive assemblies, heat exchangers) and two topical reports.

This paper presents recent activities and lessons learnt from the data collection and the results of topical analysis improving testing and multi-unit events.

Key Words: Common cause failure, CCF, ICDE

1 INTRODUCTION

Common-cause-failure (CCF) events can significantly impact the availability of the safety system of a nuclear power plants. In recognition of this, CCF data is systematically being collected and analysed in several countries. Due to the low probability of occurrence of such events it is not possible to derive a comprehensive evaluation of all relevant CCF-phenomena only from the operating experience from one individual country. Therefore, it is necessary to make use of the international operating experience from other countries using similar technology.

The usage of international NPP operating experience with CCF requires a common understanding what CCFs are and how to collect data about them. To develop such a common understanding an international common-cause failure working group was founded in 1994. This working group has elaborated the project „International Common-Cause Failure Data Exchange" (ICDE).

2 ICDE OBJECTIVES AND OPERATING STRUCTURE

The ICDE-project pursues two main aims, i.e., collect qualitative and quantitative information about CCFs in NPP, and analyse the collected data and distribute the gained insights about CCFs and methods to prevent CCFs as reports to the concerned professional audience. The objectives of the ICDE project as expressed in the *terms and reference* are to:

- provide a framework for multinational co-operation;
- collect and analyze CCF events over the long term so as to better understand such events, their causes, and their prevention;

- generate qualitative insight into the root causes of CCF events, which can then be used to derive approaches or mechanisms for their prevention or for mitigation of their consequences;
- establish a mechanism for efficient gathering of feedback on experience gained in connection with CCF phenomena, including the development of defenses against the occurrence, such as indicators for risk based inspections; and
- generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries; and
- use of ICDE data to estimate CCF parameters.

The ICDE-project is based upon a broad international cooperation (Figure 1): The countries which participate in the ICDE project operate 281 NPP units which is about 63 % of all NPP units worldwide. With a generation capacity of 275.864 MW these 281 units provide more than 70 % of the worlds' total nuclear generation capacity. The number of 281 units comprises 191 PWR, 68 BWR and 23 PHWR so the majority of NPP types is covered.

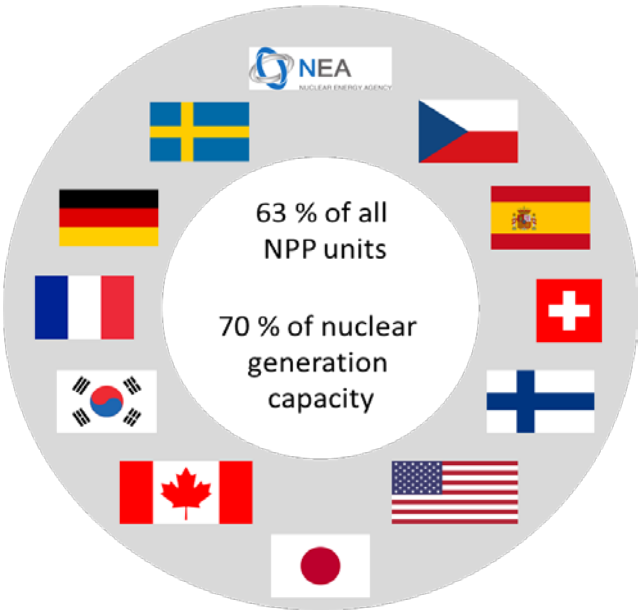

Figure 1 International cooperation and operating experience

3 ICDE ORGANISATION

The central body of the ICDE project is the ICDE Steering Group (SG) in which each participating country is represented by its national coordinator. The SG controls the project, assisted by the NEA project secretary and the Operating Agent (OA). The OA is responsible for the database and consistency analysis. The NEA Secretariat is responsible for administering the project. The SG meets twice a year on average.

The ICDE Steering Group has the responsibility to:

- Secure the financial (approval of budget and accounts) and technical resources necessary to carry out the project,
- Nominate the ICDE project chairman, to define the information flow (public information and confidentiality),
- Approve the admittance of new members,

- Nominate project task leaders (lead countries) and key persons for the Steering Group tasks,
- Define the priority of the task activities and to monitor the development of the project and task activities,
- Monitor the work of the OA and the projects quality assurance. and prepare the legal agreement for project operation.

In most countries, the data exchange is carried out through the regulatory bodies, with the possibility to delegate it to other organisations. To ensure that the data collection is performed in a consisted and comparable way in all participating countries the SG has developed and approved "coding guides" which define the format and extend of the collected information. The ICDE database is available for signatory organisations.

The project is based upon the willingness of the participants so share their operating experience; to encourage that, the participation organisations get access to the database in accordance with their own contribution to the data collection. The relevant criterion is not the total amount but the completeness of the contributed data. For example, when a country submits its operating experience with emergency diesel generators (EDG) from 1990-2010 it will get access to the complete operating experience with EDGs in that time period, irrespective of the number of NPPs that are operated in that country.

Member countries under the Phase VII Agreement of OECD/NEA and the organisations representing them in the project are: Canada (CNSC), Czech Republic (UJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), Korea (KAERI), Netherlands (ANVS), Spain (CSN), Sweden (SSM), Switzerland (ENSI) and the United States (NRC). The participation of other NEA member countries is always possible and welcome.

OECD/NEA is responsible for administering the project according to OECD rules. This means secretarial and administrative services in connection with the funding of the Project such as calling for contributions, paying expenses incurred in connection with the Operating Agent and keeping the financial accounts of the Project. NEA appoints the Project Secretariat. To assure consistency of the data contributed by the national co-ordinators the project operates through an Operating Agent (OA). The OA verifies whether the information provided by the national coordinators complies with the ICDE Coding Guidelines. Jointly with the national coordinators, it also verifies the correctness of the data included in the database. In addition, the OA operates the databank.

The SG has established a comprehensive quality assurance program: The responsibilities of participants in terms of technical work, document control and quality assurance procedures as well as in all other matters dealing with work procedures, are described in the ICDE Quality Assurance Programme (Project report ICDEPR05).

4 TECHNICAL SCOPE OF THE ICDE ACTIVITIES

4.1 Scope

The ICDE operates with a clear separation of the collection and analysis activities. The analysis results mostly in qualitative CCF information. This information may be used for the assessment of 1) the effectiveness of defenses against CCF events and 2) the importance of CCF events in the PSA framework. Qualitative insights on CCF events generated are made public as CSNI reports. The member countries are free to use the data in their quantitative and PSA related analyses.

It is intended to include in ICDE the key components of the main safety systems. The data collection and qualitative analysis result in a quality assured database with consistency verification performed within the project. The responsibilities of participants in terms of technical work, document control, and quality assurance procedures, as well as in all other matters dealing with work procedures, are described in the special ICDE Quality Assurance Program and the ICDE operating procedures.

ICDE activity defines the formats for collection of CCF events in order to achieve a consistent database. This task includes the development and revision of a set of coding guidelines describing the

classification, methods, and documentation requirements necessary for the ICDE database(s). Based on the generic guidelines, component specific guidelines are developed for all analyzed component types as the Project progresses. These guidelines are made publicly available as a CSNI technical note [1].

The scope of ICDE is intended to include the key components of the safety relevant systems. Within the data collection different types of safety relevant components are distinguished. For each component type an individual "coding guide" is developed by the steering group which defines how the data collection for that specific component type should be performed (see section 3.3 for details). An overview of the currently* covered component types is shown in Figure 2. New component types are added in case there is a corresponding interest of a participating country.

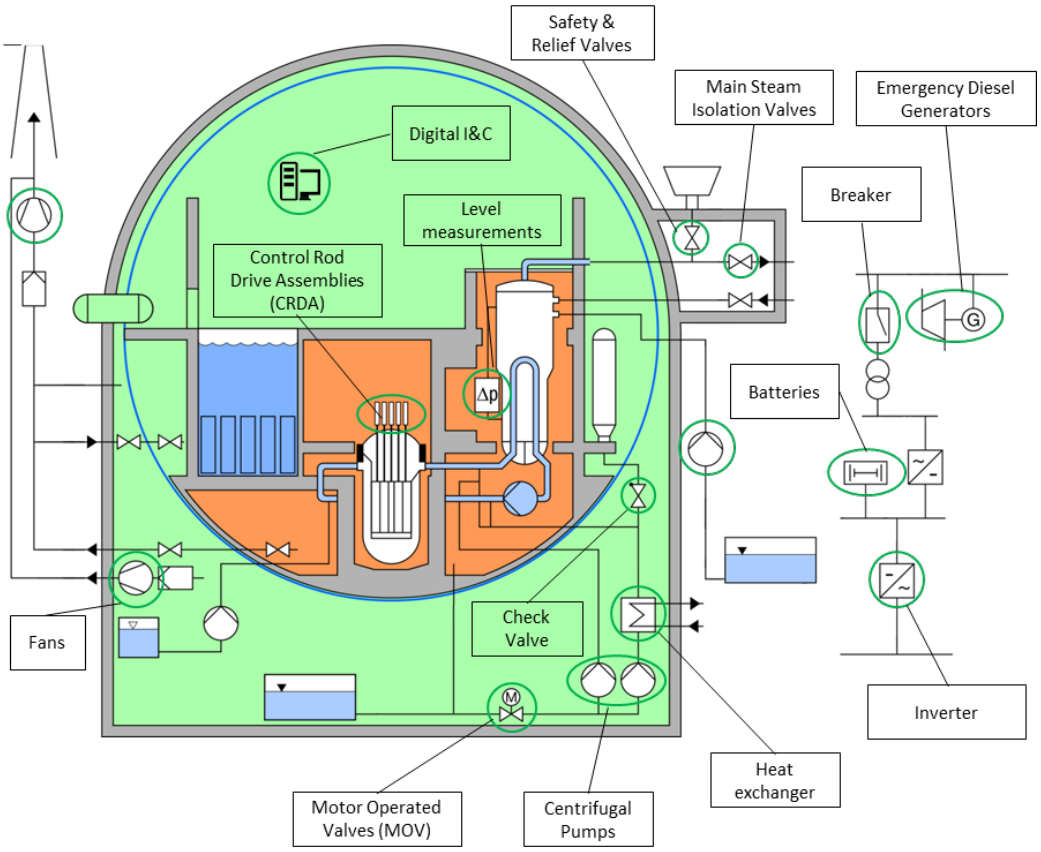

Figure 2 Technical scope of ICDE activities

4.2 Definition of Common Cause Events

Common Cause Failure Event: A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause.

ICDE data collection also includes potential CCF events, or ICDE Events, which include impairment of two or more components (with respect to performing a specific function), which exists over a relevant time interval and is the direct result of a shared cause.

4.3 Publications

The ICDE Steering Group prepares publicly available reports containing insights and conclusions from the analysis performed whenever major steps (i.e. analysis of a dataset for a certain component type like check valves) of the Project have been completed. The ICDE Steering Group assists the appointed lead person in reviewing the reports. Following this, an external review is provided by the NEA Committee

* As of November 15, 2017

on Safety of Nuclear Installation (CSNI). ICDE reporting also includes submitting papers to suitable international conferences like PSAM and PSA, and to journals. The intention is to make the lessons learnt known to the large nuclear safety audience.

The ICDE time schedules define the milestones of data collection tasks for each analyzed component group. The time schedule is reassessed and revised at each ICDE Steering Group meeting. The work starts with drafting the guidelines, getting comments, making a trial data collection, approving the guidelines, making the data exchange, resolving the remaining problem cases, and reporting.

Generally, it takes between 1.5 and 2 years from the first guideline draft to commence the data exchange itself. Furthermore, from that point it takes about 2-3 years to approving the final report. Thereafter, new exchange rounds (database updating) are possible.

The database contains general information about event attributes like root cause, coupling factor, detection method, and corrective action taken. As for the current phase VII (June 2016), data analysis and exchange have been performed for Centrifugal Pumps, Diesel Generators, Motor-operated Valves, Safety Relief Valves, Check Valves, Batteries, Level Measurements, Switching Devices and Circuit Breakers, Control Rod Drive Assemblies, and Heat Exchangers. Also, first round data collection has been performed on Fans and Main Steam Isolation Valves and has started for Digital Instrumentation and Control equipment.

4.4 Published ICDE component reports

Public final reports for Centrifugal Pumps, Diesel Generators, Motor-operated valves, Safety & Relief Valves, Check Valves, Batteries, Level Measurements, Switching Devices and Circuit Breakers, Control Rod Drive Assemblies, and Heat Exchangers have been issued in the NEA CSNI series [2]-[13], (see also: http://www.nea.fr/html/nsd/docs/indexcsni.html).

Guidelines for Fans, Main Steam Isolation Valves and Digital Instrumentation and Control equipment have been approved; those for Inverters and Cross component CCF (Asymmetric faults) are almost finalized. Also, an updated report on Centrifugal Pumps has been issued [11].

4.5 Data collection overview

An overview of the database content[†] with the number of CCF events and the number of complete[‡] and partial[§] CCF events for each component type is given in Table 1. Events are further analyzed and categorized according to the ICDE failure analysis guidelines.

Table 1 Data collection overview

Component Type	CCF Events	Percentage	Complete CCF	Partial CCF
Centrifugal Pumps	399	22,0%	51	39
Safety and Relief Valves	271	15,0%	26	36
Diesels	236	13,0%	26	18
Control Rod Drive Assembly	173	9,6%	3	24
Motor Operated Valves	172	9,5%	9	33
Level measurement	154	8,5%	7	27
Check valves	117	6,5%	14	24
Breakers	110	6,1%	8	25
Battery	77	4,3%	5	2
Heat Exchanger	55	3,0%	4	1
Fans	32	1,8%	3	0
Main Steam Isolation Valves	10	0,6%	3	0

[†] As of 15 November 2017.
[‡] Complete CCF: A common-cause failure in which all redundant components are failed simultaneously as a direct result of a shared cause (i.e., the component impairment is 'Complete failure' for all components and both the time factor and the shared cause factor are 'High').
[§] Partial CCF: A complete failure of at least two components, but not all of the exposed population, where these fault states exist simultaneously and are the direct result of a shared cause.

Digital I&C	4	0,2%	2	0
Cross-component CCF	0	0,0%	0	0
Total	1810	100%	161	229

The participating countries are gradually extending the data with more observation time and events. The frequency of observing an ICDE event in an observed population (CCF component group) is approximately 0.015/year (or <2E-6/h). This low frequency in itself justifies an international collaboration on this issue. Figure 4 shows the data collection progress, i.e. when data has been synchronized and exchanged and how the database has been expanded with new components and data exchanges over the years.

The chronological sequence of the data collection is shown in Figure 3. The graph shows how new component types were added over time as well as the continuous data collection for the existing component types.

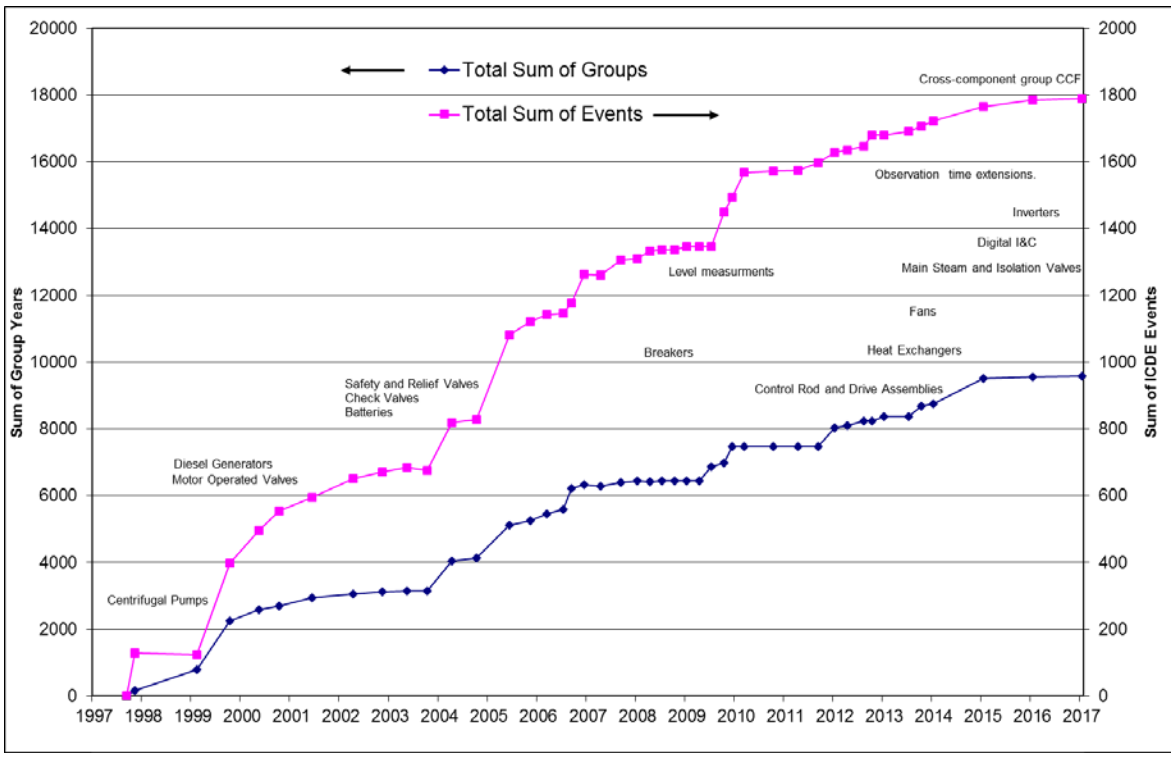

Figure 3 ICDE data collection progress

5 LESSONS LEARNT

Lessons learnt cover lessons about reporting of project results as well as technical insights from topical analysis of ICDE data. This experience has been collected in a failure analysis guide that is applied when a new component report is produced or if a new topical report is prepared. This section presents an overview of the guide and recent or ongoing applications.

5.1 Failure analysis guideline

When analyzing events, the approach to perform a failure analysis by examining failure mechanism categories, failure mechanism sub categories, and failure cause categories, and their correlations, proved to be very successful. Evaluations following this concept have revealed insights that would otherwise not have become evident. By incorporating failure analysis fields in the ICDE database, this assessment is as transparent as any other assessment being performed. The development of failure analysis provides:

- Appropriate transparency and reproducibility between component reports and the database. It is further expected that the opportunity to find new perspectives and to engage in new

development of data analysis will increase as the database content is extended with failure analysis.

- Additional aspects when conducting workshops.
- Detailed analyses of failure mechanisms that will provide valuable insights for improving defenses against the occurrence of CCF events.

An approach has been developed to perform failure analysis focused on failure mechanisms. Failure mechanisms should be considered as consequences to the failure cause. Therefore, the following steps should be performed in chronological order when performing a failure analysis:

1. Describe the failure mechanism in a few words. The failure mechanism is a history describing the observed events and influences leading to a given failure. Aspects of the failure mechanism could be deviation or degradation or a chain of consequences.
2. Specify the failure mechanism category. A failure mechanism category is a group of similar failure mechanism sub-categories, e.g., for Diesels, the Failure mechanism category "Engine damage or problems" has the following failure mechanism sub-categories
   - "Starting air or air supply valve/distributor damage",
   - "(Potential) damage of rotating or stationary parts (bearings, crankcase high pressure in crankcase etc.)",
   - "Combustion chamber problems (e.g., cylinder, piston, fuel injection nozzle, and pump damage)",
   - "Coupling (between engine and generator) damage",
   - "Combustion/Charging air problems (e.g. air intake, turbocharger damage)"
   - "Other, for example faulty operator action or maintenance error"
3. Specify the failure mechanism sub-category. Failure mechanism sub-categories are coded component-type-specific observed faults or non-conformities that have led to an ICDE event.
4. Specify the failure cause category. Failure cause categories are potential deficiencies in operation or deficiencies in design, construction, and manufacturing that made it possible for a CCF event to occur.

A list of the failure mechanism descriptions can be an easy, and yet efficient, way to summarize the type of failures for a certain scope of events.

5.2 Topical reports

Topical analyses have been performed or are under preparation for a number of topics:

- External Factors, [14] (2015, 43 events)
- Diesels all affected [15] (completed, to be published)
- Plant Modifications (Drafted, 54 events)
- Improving Testing (Drafted, 32 events)
- Multi-unit events, (Drafted, 99 multi-unit events)
- Inter-system dependencies (ongoing, 27 events)
- Pre-initiator human failure ICDE events, (ongoing)

In this paper the recently completed topical analysis results of topical analysis improving testing and multi-unit events are discussed in detail and the objectives and scope of the ongoing analysis is presented.

5.2.1 Improving Testing

The goal of the "Improving testing" topic was to identify testing inadequacies and identify ways on how to improve testing to reduce detection times and the risk of events occurring.

Identified test inadequacies among the events are:

- Extent of the test: Five events in which two events concerned operating modes and three events concerned operating conditions. The test inadequacy "Extent of test" reflect issues on plant level.
- QA of test/maintenance/modification: 30 events were assigned to this category and it was the most common category. Quality assurance (QA) of completeness and adequacy of testing were the most common issues among the sub-categories.
- Testing scope: 10 events were assigned to this category, where this category indicate that the testing did not cover all aspects on system level to prevent the event from happening.
- Performing the test: 9 events were assigned to this category. This category identifies the different types of errors which can be related to the performing the test. It focuses on instructions, use of equipment, training of staff and work control (following procedure).
- Verification of operability: 18 events were assigned to this category. This category focuses on identifying events where the operability is inadequate after activities where latent failures may occur at a real demand. The most dominating inadequacy was related to verification of operability after maintenance.

The lessons learned from the engineering aspects are:

- The test inadequacies can be divided into different categories. Some categories show a certain degree of overlap. For example, if an event is missing a step in the testing procedure this could be interpreted as a problem with testing scope, QA of completeness of test or as verification of operability after test.
- A process for quality assurance of procedures to ensure completeness, adequacy and validity of test is shown to be of high importance.
- When performing the test, it is important to verify the equipment, ensure a high degree of training of the personnel performing the test, and to have a safety culture which do not omit steps and verify the work.
- Verification of operability after test, maintenance activities and modifications are essential, especially after maintenance to prevent latent failures and occurrence of CCF.
- The actual defences that prevented event from becoming complete CCFs shows that experience feedback from other units and previous events can be a successful way to detect latent failures in time when ordinary testing may not identify certain failure mechanisms.

5.2.2 Multi-unit events

The goal of the "multi-unit event" topic was to analyse events affecting multiple reactor units by identifying multi-unit dependencies and CCF defence aspects related to such events. The topical report includes 87 multi-unit events involving a total of 192 ICDE events affecting multiple units at one or several sites. These reported ICDE events were classified with respect to; degree of multi-unit correlation expressed by internal/external correlation factors; simultaneity between the events; and by degree of severity. The observed multi-unit events were classified as:

- **Internal factors** (Shared cause and fleet CCF events) with Organizational, Human or Identical design correlation factors.
- **External factors** (Shared environment or physical connection) with Proximity or Shared Structures, Systems and Components (SSCs) correlation factors.

Multi-unit events were observed for a wide range of component types. Diesels and Centrifugal pumps were most common, i.e., more than 50% of events involved these types. Root cause design and deficiencies in hardware were most prominent. Deficiencies in operation was almost equally common as hardware issues. About 20% of the events were observed with environmental deficiencies. 9 events, about 10% of the multi-unit events, were complete multi-unit CCF events. The conclusions drawn from the analysis of multi-unit events, divided by internal/external correlation factors, were:

Insights of the internal factors

- The most common correlation factor was "Identical design". Events were correlated through same design of components/systems, operating environment, installation. Also, some events were correlated using same unsuitable grease/lubrication. The correlation factor "Human" involve issues with maintenance actions, such as cleaning (grease), improper fixing. The correlation factor "Organisational concern mainly incorrect procedures (both test and maintenance).
- All the identified fleet CCF events were correlated by internal factors.
- Five of the nine complete CCF events had an internal correlation factor, three event with identical design and two correlated by organisation. Several types of improvements were suggested, such as improved design and revising procedures.
- Feasible defence strategies against failures developing into complete CCFs are well-functioning testing procedures, maintenance procedures, operating experience feedback, skilled personnel etc. Adequate and robust system/component design is the fundamental defence against complete CCFs. If the event severity is considered, it can be concluded that for most of the events adequate defences exist, but for 15 events no actual defence could be identified.
- The most common improvement areas were Design of component, Surveillance of component or Maintenance procedure for component, Testing procedure and Management system of plant.

Insights of the external factors

- A total of 14 events were dependent through external factors, where 10 of these events were correlated to *"Shared SSCs"*.
- Four of the nine complete CCF had an external correlation factor, more specifically shared SSCs. As defence, better design of water intake was suggested for three events and improved maintenance procedure for the fourth event.
- Improvement area *Design of system or site* involved both internal and external factor events, but this area was suggested for about half of the events with an external correlation factor. Area *Surveillance/Maintenance* was also common.
- The external factor multi-unit events have some overlap with report [12], which focused on single unit external factors.

5.3 Ongoing topical analyses

5.3.1 Plant Modifications (ongoing, 54 events)

The objective is to study events in which failures occurred due to modifications in systems, components or procedures, etc.

The selected CCF events are of wide variety but have one common denominator, i.e. modification. The type of modifications of interest were design modifications of components and systems, modification of settings, backfitting of components with new or modified designs, and replacement of components with identical design. Also, events that occurred due to modified test procedures are included.

5.3.2 Inter-system dependencies

The objective of this topical report was to study events with intersystem dependencies, i.e. events were a single CCF failure mechanism affects components in more than one different system or affected more than one different safety function. The workshop results are presented using the following classification.

- Actual intersystem dependency.
- Partial/Incipient intersystem dependency.
- Potential intersystem dependency.
- Inter-CCCG[**] dependency events. Some of the included events showed that only multiple CCF groups in the same system was affected. These are not ordinary intersystem events, but are interesting since these involve dependencies between CCF groups which are not specifically modelled in a PRA.

5.3.3 Pre-initiator human failure ICDE events.

The goal of the workshop will be to review operational plant experience and possibly find defenses against human failure events (HFEs). Analysis for pre-initiator HFEs will include:

- Identify activities/actions resulting in dependent pre-initiator HFEs
- Identify involved PSFs (performance shaping factors) for the specific dependent pre-initiator HFEs

6 DISCUSSION

What can be said is that the ICDE has changed the view of CCFs a great deal. For instance, determination of the fact that the most common cause of complete CCFs seems to be human action as a part of operation or design, rather than manufacturing deficiencies, would not have been possible without deep plant data collection and combining of information from many sources.

Maybe the most important generic lesson is that it is worth forming specialized data exchange projects like ICDE. This, however, requires first the will of several countries to form a critical mass by combining their operating experience efforts; second, it requires national efforts to collect lower level data than those made publicly available as LER or IRS reports; third, it requires the forming of a legal framework to protect this proprietary data and, fourth, a long term commitment to consistently continue and develop the activity.

OECD NEA and ÅF industry, as the Operating Agent, have provided the means to run the international dimension of the ICDE; however, national efforts are the key to the success of any project that relies on operating experience. The success of the ICDE has given a birth to several similar types of projects, among which are the CODAP for pipe failure events and the OECD-FIRE for NPP fire events.

More information about ICDE may be obtained by visiting the CSNI report site: http://home.nea.fr/html/nsd/docs/indexcsni.html, or the Operating Agent website: https://projectportal.afconsult.com/ProjectPortal/icde or by contacting the responsible OECD administrator.

[**] Common-Cause Component Group

References

[1.] ICDE General Coding Guidelines [NEA/CSNI/R(2004)4], January 2004.

[2.] Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(99)2], September 1999.

[3.] Collection and analysis of common-cause failure of emergency diesel generators [NEA/CSNI/R(2000)20], May 2000.

[4.] Collection and analysis of common-cause failure of motor-operated valves [NEA/CSNI/R(2001)10], February 2001.

[5.] Collection and analysis of common-cause failure of safety valves and relief valves [NEA/CSNI/R(2002)19]. Published October 2002.

[6.] Collection and analysis of common-cause failure of check valves [NEA/CSNI/R(2003)15], February 2003.

[7.] Collection and analysis of common-cause failure of batteries [NEA/CSNI/R(2003)19], September 2003.

[8.] Proceedings of ICDE Workshop on the qualitative and quantitative use of ICDE Data [NEA/CSNI/R(2001)8], November 2002.

[9.] Collection and analysis of common-cause failure of switching devices and circuit breakers [NEA/CSNI/R(2008)01], October 2007.

[10.] Collection and analysis of common-cause failure of level measurement components [NEA/CSNI/R(2008)8], July 2008.

[11.] Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(2013)2], June 2013.

[12.] Collection and analysis of common-cause failure of control rod drive assemblies [NEA/CSNI/R(2013)4], June 2013.

[13.] Collection and analysis of common-cause failure of heat exchangers [NEA/CSNI/R(2015)11], August 2015.

[14.] ICDE Workshop - Collection and Analysis of Common-Cause Failures due to External Factors [NEA/CSNI/R(2015)17], October 2015.

[15.] ICDE Workshop - Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Population, 2015. NEA/CSNI/R(2017)8, August 2017.