RECENT INSIGHTS FROM THE INTERNATIONAL COMMON CAUSE FAILURE DATA EXCHANGE (ICDE) PROJECT

Albert Kreuser[a], Gunnar Johanson[b]

[a] Gesellschaft für Anlagen- und Reaktorsicherheit(GRS) gGmbH, Cologne, GERMANY
[b] ÅF Industry, Stockholm, SWEDEN

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 that include CCF modelling. Because CCF events are typically rare events, most countries do not experience enough CCF events to perform meaningful analyses. Data combined from several countries, however, yields sufficient data for more rigorous analyses. The qualitative insights gained from the analysis of CCF events are made available by reports that are distributed without restrictions. Database requirements are specified by the members of the ICDE Project working group and are fixed in guidelines. Each member with access to the ICDE database is free to use the collected data. It is assumed that the data will be used by the members in the context of PSA/PRA reviews and application.

The ICDE project has published meanwhile eleven reports on collection and analysis of CCF events on 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 on emergency diesel generator CCF impacting entire exposed population.

ICDE has changed the views to CCFs a great deal. Many insights would not have been possible to identify without a deep plant data collection and combining information from many sources. This paper discusses generic lessons how to create and operate such projects to form critical masses of operating experience and insights from recent analysis of CCF events.

I. INTRODUCTION

Common-cause-failure (CCF) events can significantly impact the availability of safety systems of nuclear power plants. In recognition of this, CCF data are systematically being collected and analysed in most countries. A serious obstacle to the use of national qualitative and quantitative data collections by other countries is that the criteria and interpretations applied in the collection and analysis of events and data differ among the various countries. A further impediment is that descriptions of reported events and their root causes and coupling factors, which are important to the assessment of the events, are usually written in the native language of the countries where the events were observed.

To overcome these obstacles, the preparation for the international common cause data exchange (ICDE) project was initiated in August of 1994. Since April 1998, the OECD/NEA has formally operated the project. The current phase VII has an agreement period that covers years 2015-2018. 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), Korea (KAERI), Spain (CSN), Sweden (SSM), Switzerland (ENSI) and United States (NRC).

The objective of this paper is to give generic information about the ICDE activities and the lessons learnt from recent analysis of CCF events in the ICDE database.

II. ICDE OBJECTIVES AND OPERATING STRUCTURE

The objectives of the ICDE project (denoted later as the Project) are:

- to provide a framework for a multinational co-operation;
- to collect and analyze CCF events over the long term so as to better understand such events, their causes, and their prevention;
- to generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences;
- to establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defenses against their occurrence, such as indicators for risk based inspections; and
- to record event attributes to facilitate quantification of CCF frequencies when so decided by the member countries of the Project.

The ICDE Steering Group (SG) controls the Project with assistance from the NEA project secretary and the Operating Agent. The Operating Agent is responsible for the database and consistency analysis. The NEA Secretariat is responsible for administering the project on behalf of the OECD. The ICDE operating structure and documents related to it are depicted in Figure 1.

Running an international project requires funding and consequently the participating countries make yearly an agreed ICDE contribution to the NEA for reimbursement of the costs of the Operating Agent and the OECD NEA Secretariat. In addition, each participant bears all other costs, like the ones for data collection and national analysis, associated with participation in the Project. These costs are generally much higher than the costs of running the Operating Agent. Moreover, the in-kind principle is followed in the data exchange where each country gets the dataset corresponding to its own data sent to the Operating Agent. Thus, just participating and paying the fees does not lead to directly receiving any data without a member's own data collection and submittal effort.

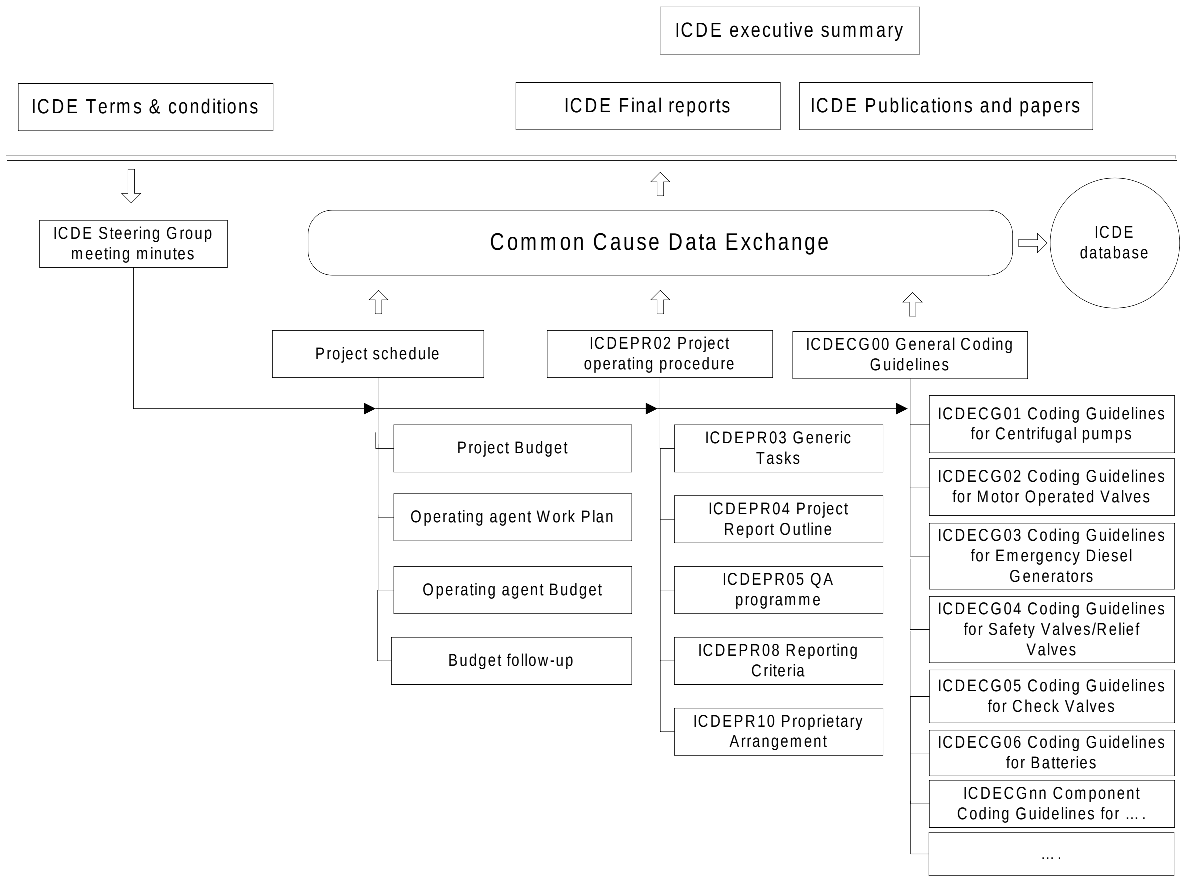

Figure 1. Operating procedure documents overview.

The SG meets twice a year on average. Its responsibilities include the following types of decisions: to secure the financial (by approval of budget and accounts) and technical resources necessary to carry out the project; to nominate the ICDE project chairman; to define the information flow (public information and confidentiality); to approve the accession of new members; to nominate project task leaders (lead countries) and key persons for the Steering Group tasks; to define the priority of the task activities; to monitor the development of the project and task activities; to monitor the work of the Operating Agent & quality assurance and to prepare the three-year legal agreements "Terms and Conditions", see Figure 1, for project operation. The ICDE experience tells that such a legal agreement completed by internal operating rules and summary presentations are vital prerequisites of mutual understanding and a functioning framework for a long-term internal co-operation with many countries involved.

An agreement and an Operating Agent do not alone guarantee good quality results, but data collection and analysis has to be organized at national level. In most countries, the data exchange is carried out through the regulatory bodies. They often delegate this to other organizations, since arriving at the information required by ICDE requires access to plant maintenance data. That data is normally proprietary. Consequently, the ICDE database is only available for signatory organizations and restricted by proprietary rights. The only possibility to get access to the working material is to actively take part in the data exchange.

OECD/NEA is responsible for administering the project according to OECD rules. This means secretarial and administrative services. Issuing publicly available ICDE reports, calling for member contributions/fees, paying expenses incurred in connection with the Operating Agent activities and keeping the financial accounts of the Project are examples of these activities. NEA appoints the Project Secretary from amongst its administrators.

To assure consistency of the data contributed by the national coordinators, the project operates through an Operating Agent. The Operating Agent verifies whether the information provided by members complies with the ICDE Coding Guidelines. It also verifies the correctness of the data included in the database jointly with the national coordinators. In addition the Operating Agent operates, and develops if necessary, the ICDE databank. ÅF Industry (previously ES Konsult) in Sweden is currently running the Operating Agent.

III. TECHNICAL SCOPE OF THE ICDE ACTIVITIES

III.A. ICDE operation

The ICDE operates with a clear separation of the collection and analysis activities. In the first stage of the project, emphasis has been on the collection of data. The analysis results mostly in qualitative CCF information. It 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. The 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 technical work, document control and quality assurance procedures as well as all other matters dealing with work procedures are described in a special ICDE Quality Assurance Program and the ICDE operating procedures.

The 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].

III.B. ICDE reporting

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 on Safety of Nuclear Installation (CSNI). ICDE reporting also includes papers to suitable international conferences like PSAM and PSA, and journals. The intention is to make the lessons learnt known to a 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 commencing 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. The breakdown of resulted ICDE events in the database, i.e. events involving at least incipient common cause characteristics, of various components is shown in Table 1**.** Special emphasis is given on CCF events in which each component fails completely due to the same cause and within a short time interval. These events are called "Complete CCF".

Table 1 Number of ICDE events

Component	No. of events in component report	No. of ICDE events with complete CCF in component report	No. of events in database (June 2016)	Data amount change since component report
Centrifugal pumps	353[i2] (125[i1])	42[i2] (19[i1])	391	11%
Diesels	224[i3] (106[i1])	23 [i2] (17[i1])	229	2%
MOVs	86	5	170	98%
SRVs	149	14	271	82%
Check valves	94	7	116	23%
Batteries	50	3	77	54%
Breakers	104	6	107	3%
Level measurement	146	6	154	5%
Heat Exchangers	46	4	55	20%
CRDA	169	-	172	2%
MSIV	-	-	10	-
Fans	-	-	32	-
Digital I&C	-	-	4	-
Inverters	-	-	-	-
Cross component CCF	-	-	-	-
Total	1421	110	1788	26%

[i1] Issue 1, [i2] Issue 2 [i3] Issue 2 ongoing, not published

III.C. 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 and those for Inverters and Cross component CCF (Asymmetric faults) are almost finalized. Also, an updated report on Centrifugal Pumps has been issued [11].

Until June 2016, 1421 ICDE events had been analyzed and reported. The total number of event records collected in the database for the analyzed component types is 1742. The breakdown into the various components is shown in Table 1. The third column shows the numbers of events in which each redundant component failed completely due to the same cause and within a short time interval. Events are further analyzed and categorized according to the ICDE failure analysis guideline, see Section IV.A.

III.D. ICDE Data status

ICDE Observation overview across all ICDE components can be summarized by the following figures. Figure 2 illustrates the overall ICDE observation by presenting the total number of events per year together with the total number of group years observed (per year). The participating countries are gradually extending the data with more observation time and events. Figure 3 presents a trend for the ICDE event rate, including all events falling inside the ICDE event definition, i.e. both complete as well as potential CCF events. Also the 10 periods (years) moving average is indicated in Figure 3. The systematic data exchange started 1990, events reported before 1990 are reported for qualitative use. The frequency to observe an ICDE event in an observed population (CCF component group) is approximately 0.015/year (or <2E-6/h). This low frequency justifies an international collaboration on this issue in itself.

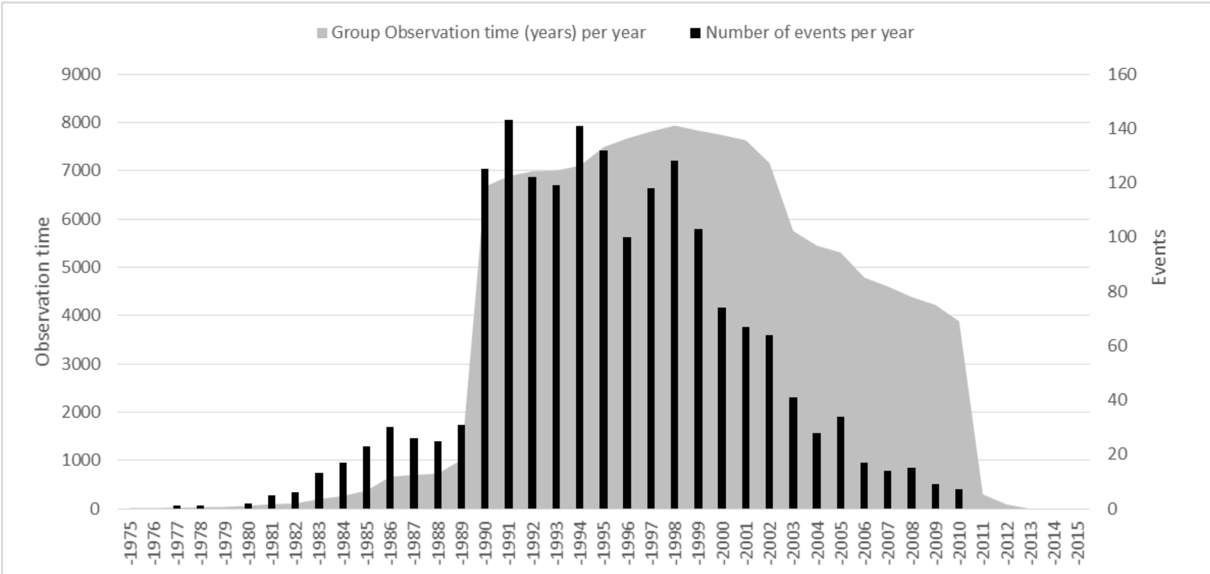

Figure 2. ICDE observation overview.

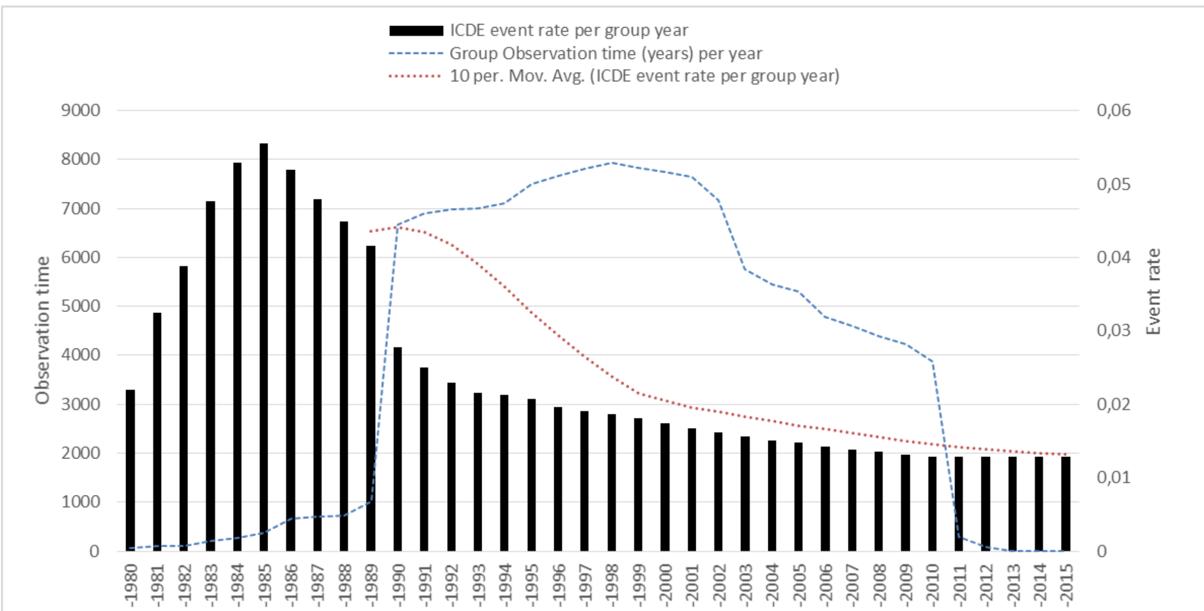

Figure 3. ICDE event rate.

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.

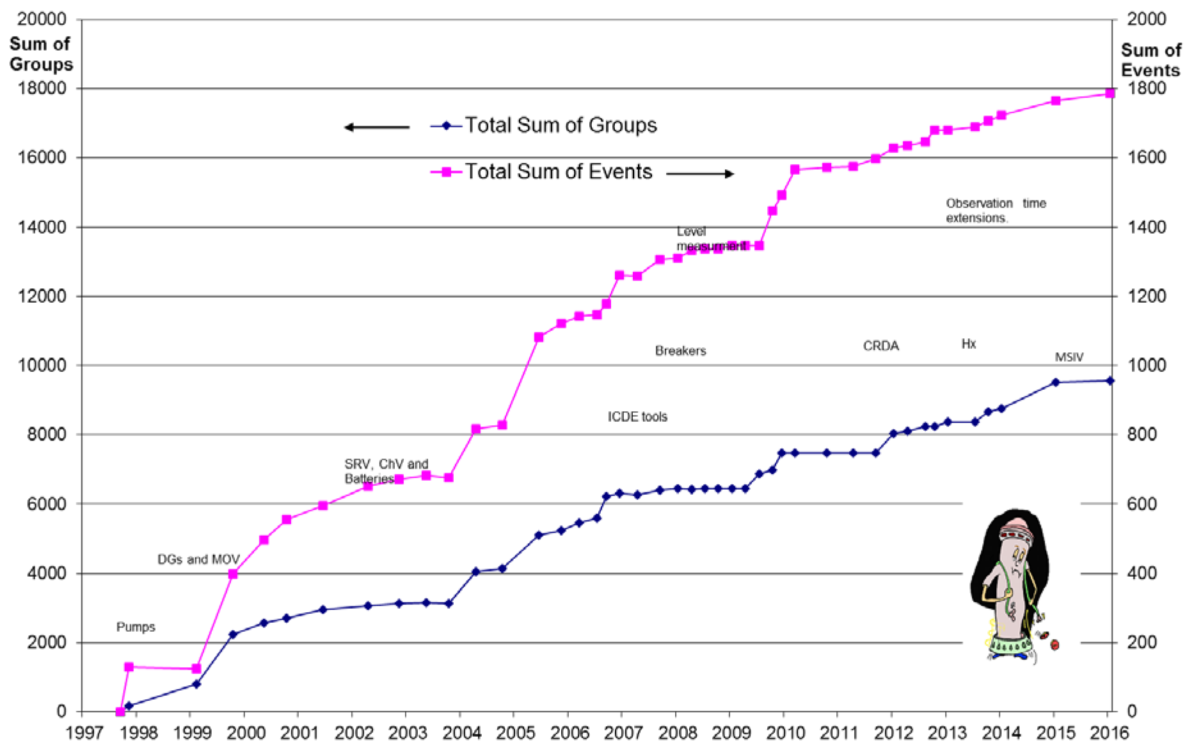

Figure 4. ICDE data collection progress.

IV. LESSONS LEARNT

Lessons learnt cover lessons about reporting of project results as well as technical insights from topical analysis of ICDE data. The component report follows the general format to present qualitative insights from the data set. This has gradually been improved as more failure analysis has been performed. This experience has been collected in a failure analysis guide that is applied when a new component report shall be produced or if a new topical report are prepared. This section presents an overview of the guide and recent or ongoing applications.

IV.A. The failure analysis guideline

When analyzing events in the current format of the component reports, 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 which would otherwise not have become evident. By incorporating failure analysis fields in 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 of finding new perspectives and development of data analysis will increase with the database content being extended with the failure analysis.
- Additional aspects when conducting workshops.
  Detailed analyses of failure mechanisms which will provide valuable insights for improving defences against the occurrence of CCF events.

The work procedure shall support the ICDE SG when analysing events for the reports where an approach has been developed to perform a 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 chronologically 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 a 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
   a. "Starting air or air supply valve/distributor damage",
   b. "(Potential) damage of rotating or stationary parts (bearings, crankcase high pressure in crankcase etc)",
   c. "Combustion chamber problems (eg cylinder, piston, fuel injection nozzle and pump damage)",
   d. "Coupling (between engine and generator) damage",
   e. "Combustion/Charging air problems (e.g. air intake, turbocharger damage)" and
   f. "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 which have led to the ICDE event.
4. Specify the failure cause category. Failure cause categories are potential deficiencies in operation or deficiencies in design, construction and manufacturing which rendered possible a CCF event to occur.

A list of the failure mechanism descriptions can be an easy, but yet efficient, way to summarize the type of failures for a certain scope of events. An example is given in section IV.C of this paper.

IV.B. 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 (ongoing, 54 events)
- Improving Testing (ongoing, 32 events)
- Multi-unit events, (ongoing, 99 multi-unit events)
- Pre-initiator human failure ICDE events, (Proposed for 2017)

In this paper the recently completed topical analysis report on Diesels all affected is discussed in detail and the objectives, scope and preliminary results of the ongoing analysis is presented.

IV.C. Topical analysis on Diesels all affected

IV.C.1. Overview

This topical analysis is completed in the ICDE steering group and the report is to be published. The report summarizes the workshop results and presents an overview of the exchange of CCF data among several countries of diesel failures impacting entire exposed populations, so called "all affected" diesel failures. "All affected" diesel failures involves events where all diesels in an exposed population either failed or were degraded or showed an incipient impairment due the same cause.

The workshop format included questions like

- If the event is not a complete CCF (for definition see chapter III.B):
  - Can you identify any actual defences that prevented all components to fail?
  - Can you identify any areas of improvement in order to prevent the event from happening again?
- If complete CCF:
  - Can you identify any possible defences or areas of improvement that could have prevented all components to fail?

The most common answer to the question "what have or could have prevented all components to fail" was that the failure was slowly developing over time and was therefore detected before all components failed. This indicates that there is a good chance that the diesel failures are possible to detect "in time".

It was also established that specifying the failure mechanism was a good start in the analysis process. The failure mechanism describes the observed event and influences leading to a given failure.

The table below is taken from the ICDE workshop report on diesels impacting entire exposed population where examples of concluded failure mechanisms for "Complete CCF" are listed. In addition, for a better general view, the mechanisms in the report where sorted by relevant mechanism groups (derived from the root cause codes).

The ICDE failure analysis guideline will be published as a new appendix in the coming update of the ICDE general coding guidelines.

Table 2 Failure mechanism descriptions

Failure mechanism examples for "Complete CCFs"	**Mechanism group**
Cracks in numerous relay sockets were induced by vibrations in the EDG rooms resulting failure of diesel load control	Hardware
ESW strainers were deformed allowing fish to plug ESW components	
External corrosion on cooling pipes due to penetration of rain water because of a non-leak-proof EDG building	
Lockout relay of both EDG output breakers were found sticking (not tripping when required)	
Mechanical fatigue causing pin rupture in pumps that provide fuel to diesels	
Short circuits in two diodes in the rectifier bridge caused a protective fuse to blow, which caused the engine of the EDG to speed during a surveillance test	
A repair work at a reactor protection system cubicle caused a spurious signal that started the DGs. DGs stopped when the signal disappeared.	Human
Erroneous test procedure led to the operator to lock the automatic start-up of both EDG, which was not according to Technical Specification requirements.	
Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply	
Improper switch position - the inhibit keys for under voltage protection were in place and the sensor channels for both vital buses were bypassed.	
Incorrect installation of the flow control valves due to procedural inadequacies, inattention to detail and inadequate skills.	
Pollution of the air supply due to sandblasting outside the Diesel building	

IV.C.2. Areas of improvement and preventions for all effected events

Six categories of improvements are defined in

Table 3. The events were reviewed to determine where the improvement categories proposed in the workshop format could be applied. Each event could be assigned to multiple improvement categories. It resulted in 135 events with one selected category, 46 events with 2-4 selected categories and seven events with no selected categories at all.

In Table 3 it could be seen that the most common assigned category was “Maintenance or testing of component” (34%). Many of these events involve improper re-installations or re-assemblies after testing/maintenance. For example, in one event the governors were incorrectly replaced after testing/maintenance. Suitable prevention for this kind of failure is improved test/maintenance procedures which includes checks after finished test/maintenance. Approximately 15% of the events were concluded with this type of prevention. Within this improvement category the following additional noteworthy insights have been established:

- When planning maintenance activities and procedures the function of ancillary equipment has to be taken into account.
- For events which include clogging of oil filters a preventive action could be to add an “oil filter non-clogging verification” on the periodic test procedure consisting of a pressure drop measurement.
- Increased redundancy of the level measurements in the diesel fuel tanks combined with staggered testing can detect LM failures such as miscalibrations.

Table 3 Distribution of identified improvement categories

Improvement category	**No. of events**	**Percent**
a – Design of system or site	15	8,3%
b – Design of component	51	28,2%
c – Surveillance of component	15	8,3%
d – Maintenance or testing of component	61	33,7%
e – Operation of component	10	5,5%
f – Management system of plant[1]	29	16,0%
Total	181	100,0%

Also the improvement category “Design of component” was common among the events (28%). Improper design of different piece parts such as cooling pipes, three-way-valves (gap rod/valve) and exhaust damper linkage seems to be the problem for many events.

Among the 29 events (16%) which were assigned “Management system of plant”, improved QA of the vendor was pointed out several times. Regarding one event better instructions about screwing torque of lock-nut for the three-way valve from the manufacturer would have prevented the event from happening (the lock-nut was not tightened

[1] QA of vendor, spare parts management, training of personnel, sufficient resources/staff etc.

enough). This implies that “QA of vendor” not only involves quality assurance of the actual product but also that the product information delivered together with the product is sufficient.

Examples of events assigned with category “Design of system or site” are accordingly design errors such as corrosion in cooling pipes due to penetration of rain water because of a non-leak-proof EDG building or inadequate vibration tolerant design leading to cracks in the cooling system. Regarding building designs, it is important to implement state-of-the-art practices to handle possible weather phenomena such as rain water.

Examples of events assigned with category “Surveillance of component” are blockage in heat exchanger tubes (primarily corrosion nodules) and unusual high oil consumption which led to low oil level and stopping of the engine. Monitoring the flow in cooling pipes, the oil consumption and also the diesel fuel supply could be an appropriate improvement for these types of events. However, if increasing the number of monitors and alarms in the control room the risk of overlooking important alarms should be considered.

One example of an event assigned with category “Operation of component” is over temperature of diesel due to dirt deposition on heat exchanger due to high iron content of well water. In the concerned plant it is possible to use river or well water depending on the circumstances, and with regard to this event, operation with river water could have prevented the event from happening. As lesson learnt from this event it can be derived that controlling the water chemistry of the cooling water is important.

The most common answer (23%) to the question “what have or could have prevented all components to fail” was that the failure was slowly developing over time and was therefore detected before all components failed.

For one event (welding with in other room activated fire suppression system in the common basement under the diesel rooms where cables are installed) it is concluded that consequent spatial separation of redundancies including ancillary equipment (cables in this case) would have resulted in a less substantial event. Another preventive action for the same event would be to seal possible fume transfer routes (wall penetrations) during maintenance activities.

Another noteworthy comment is that only one event was concluded as “Nothing happened because the problem was detected by failure in other unit at the same site”. This indicates the importance of informing other units and plants when an event has occurred, as a preventive action.

25% of the events were left without any answer to this workshop question.

IV.D. Ongoing topical analyses

IV.D.1. Plant Modifications (ongoing, 54 events)

In accordance with the objective of the ICDE project to generate qualitative insights regarding the root causes of CCF events which can be used to derive approaches for their prevention, a workshop on CCF events with “failures due to modifications” was performed during the ICDE Steering Group meeting in May 2014. The objective was to study events where 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, systems, modification of settings, backfitting of components with new or modified design and replacements of components with identical design. Also, events that occurred due to modified test procedures are included.

The distribution of involved modifications is presented in Table 4. The most common modification was “Backfitting with new/modified design” (62%) followed by “Modifications related to maintenance/test” (32%).

Table 4 Distribution of involved modifications.

Involved modification	**No. of events**	**Percentage**
Backfitting with new/modified design	33	62%
Main component	4	8%
Sub-component	18	34%
I&C	10	19%
Other	1	2%
Replacement with identical design	1	2%
Main component	1	2%
Other/unknown	2	4%
Modifications related to maintenance/test	17	32%
Total	53	100%

The most common CCFs due to modifications, based on the engineering aspects of the collected events, involves a design modification or a modification of settings. Possible preventions from happening again include improvement of design of component, testing procedure following modification and management system of plant. Important CCF defence aspects are design, testing (post modification and revised procedures) and QA of manufacturer.

IV.D.2. Improving Testing (ongoing, 32 events)

A workshop about CCF events related to improving testing and test procedures was performed during the 39th ICDE meeting in October 2014. The objective was to study events where any fault states or impairments could not be detected in normal recurrent tests because the scope of tests was insufficient or no appropriate tests existed.

The workshop included 32 ICDE events involving events where the testing procedures were inadequate. The aim is to find recommendations on how to improve testing to reduce detection times and the risk of events occurring. Three events were during the analysis excluded and three other events were identified to be questionable if they should belong to the ordinary PSA component boundary.

The overall conclusion from the summary of the engineering aspects is that the workshop theme “improving testing” is not completely covered in the answers of the working groups.

Nevertheless, several important findings have been identified. About 50% of the events were detected outside of normal periodic testing and planned inspections. Eight events were marked as multi-unit events and five events showed deficiencies in safety culture.

When looking at possible area of improvement for the event from happening again, three areas are more frequent in the results. These are testing procedure (38%), design of component (20%) and management system of plant (15%).

The aspects of inadequacies in the testing procedures concern:

- Lack of appropriate testing procedures
- Validity and extent of tests (e.g. include all operating modes, emergency conditions)
- Updating testing procedures after modifications
- Processes to ensure completeness and quality of tests (consistency between Operating rules and maintenance tests)
- Use of adequate testing equipment
- Check of calibration instruments and settings

IV.D.3. Multi-unit events, (ongoing, 99 multi-unit events)

A workshop about multi-unit CCF events was performed during the 40th ICDE meeting in May 2015. The objective was to study events that occurred at multiple plants at the same site where a multi-unit dependency existed between the events.

The initial key-word search for multi-unit events resulted in 35 multi-unit event *groups* (a total of 80 ICDE events) to be included in the workshop. A multi-unit event group consists of individual events of the same type that share a multi-unit dependency.

The overall conclusion from the summary of the engineering aspects is that the workshop theme on "multi-unit events" concerning multi-unit dependencies and CCF defence aspects is not conclusive. The lack of multi-unit events with physical dependencies is apparent and more events of this type should be studied. This would need a more detailed screening of the ICDE database.

The multi-unit classification shows that most of the events are site events occurring within 1 year. Also, 8 of the multi-unit event groups are multi-site events.

However, several important findings have been identified, for example, actual defences that prevented all components to fail and possible defences to prevent the events from happening again.

Actual defences: 15/35 multi-unit event *groups* prevented by ordinary testing. 5 multi-unit event groups were failures slowly developing in time and detected in time. Another example: Operating experience feedback from other plant led to an inspection, which revealed the problem. The identified actual successful defences against multi-unit CCFs include adequate test and maintenance procedures, and inspections. If the event severity is taken into account, it can be concluded that for most of the events adequate defences exist.

Possible defences: Three event groups were complete CCF and for these events, possible defences were proposed. The first event, where wrong settings for the relief valve due to incorrect engineering judgement and identical maintenance actions resulted into a complete CCF. As defence, it was proposed to introduce a process to ensure completeness, quality and validity of maintenance procedures and performing verification of operability after maintenance. The next event, where both trains of both units charging pump service water pumps became air bound. Underwater diving maintenance activities on one units circulating water and service water lines was identified as the source of the air. As defence, it was proposed to change the maintenance procedure. The last event, where the design of components led to insufficient position of the nozzles for level measurement, which resulted in too high level indication. The event was a complete CCF detected outside planned test and the components were not capable of performing its required function. The event led to design modifications (re-installation at correct position for low-level measurement). Test under real demand conditions would have revealed the problem. As defence, a change of testing procedures was suggested.

Candidates for PRA site modeling: Three event groups were assessed as candidates for PRA site modeling. The first candidate shared safety-systems between two units. For this event, the system design in combination with water passing a non-return valve led to warming of suction legs of both emergency boiler feed pumps. The second candidate shared two diesels between the two units. For this event, air was trapped in the governor compensation system which caused vibrations and resulted in operation in a degraded state. The final candidate had a multi-unit dependency through a shared connection, i.e. connected supply lines (same piping), and during maintenance activities, both trains of both units were effected.

IV.D.4. Pre-initiator human failure ICDE events, (Proposed for 2017)

The goal of the workshop would be to review operational plant experience and possibly find defences against human failure events (HFEs). The workshop would focus on identifying and understanding pre-initiators HFEs, e.g., human failure mechanisms and its root causes. Pre-initiator HFEs are in the HRA terminology denoted as "Category A events". Category A events (actions) represent alignment/configuration errors following testing or maintenance, and miscalibration are of particular significance. Event candidates have been identified within the diesel population. Based on the HRA good practices, NUREG-1792, for identification of pre-initiator human actions, the following analysis activities for pre-initiator HFEs are included in the scope of an ICDE workshop:

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

V. DISCUSSION

What can be said is that the ICDE has changed the views to CCFs a great deal. For instance, the fact that causes for complete CCFs seem to be mostly human actions as a part of operation or design rather than manufacturing deficiencies would not have been possible to identify without a deep plant data collection and combining 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 firstly the will of several countries to form a critical mass by combining their operating experience efforts, secondly national efforts to collect lower level data than made publicly available as LER or IRS reports, thirdly forming a legal framework to protect this proprietary data and fourthly a long term commitment to consistently continue and develop the activity.

OECD NEA and ÅF industry as the Operating Agent have provided means to run the international dimension of the ICDE, but national efforts are the key to the success of any project relying on operating experience. The success of ICDE has given a birth to several similar types of projects, among which are the CODAP for pipe failure events and 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, the Operating Agent website: https://projectportal.afconsult.com/ProjectPortal/icde or contacting the responsible OECD administrator.

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. To be published by CSNI.