Nuclear Safety
NEA/CSNI/R(2019)3
June 2019
www.oecd-nea.org

Summary of Phase VII of the International Common-Cause Data Exchange Project of Nuclear Power Plant Events

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CSNI/R(2019)3

Unclassified

English text only

4 June 2019

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Summary of Phase VII of the International Common-Cause Data Exchange Project of Nuclear Power Plant Events

JT03448435

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 36 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 33 countries: Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission and the International Atomic Energy Agency also take part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally sound and economical use of nuclear energy for peaceful purposes;
- to provide authoritative assessments and to forge common understandings on key issues as input to government decisions on nuclear energy policy and to broader OECD analyses in areas such as energy and the sustainable development of low-carbon economies.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management and decommissioning, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) is responsible for NEA programmes and activities that support maintaining and advancing the scientific and technical knowledge base of the safety of nuclear installations.

The Committee constitutes a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development and engineering, to its activities. It has regard to the exchange of information between member countries and safety R&D programmes of various sizes in order to keep all member countries involved in and abreast of developments in technical safety matters.

The Committee reviews the state of knowledge on important topics of nuclear safety science and techniques and of safety assessments, and ensures that operating experience is appropriately accounted for in its activities. It initiates and conducts programmes identified by these reviews and assessments in order to confirm safety, overcome discrepancies, develop improvements and reach consensus on technical issues of common interest. It promotes the co-ordination of work in different member countries that serve to maintain and enhance competence in nuclear safety matters, including the establishment of joint undertakings (e.g. joint research and data projects), and assists in the feedback of the results to participating organisations. The Committee ensures that valuable end-products of the technical reviews and analyses are provided to members in a timely manner, and made publicly available when appropriate, to support broader nuclear safety.

The Committee focuses primarily on the safety aspects of existing power reactors, other nuclear installations and new power reactors; it also considers the safety implications of scientific and technical developments of future reactor technologies and designs. Further, the scope for the Committee includes human and organisational research activities and technical developments that affect nuclear safety.

Table of contents

Executive summary

Common-cause failure (CCF) events can significantly impact the availability of safety systems of nuclear power plants. For this reason, the International Common-Cause Failure Data Exchange (ICDE) project was initiated by several countries in 1994. Since 1997, it has been operated within the Nuclear Energy Agency (NEA) framework, and the project has successfully operated over seven consecutive terms. The eighth term of the joint database ICDE project (2019-2022), organised under the NEA Committee on the Safety of Nuclear Installations (CSNI), began this year and the ten members of this eighth term of the ICDE are: Canada, the Czech Republic, Finland, France, Germany, Japan, the Netherlands, Sweden, Switzerland and the United States. The Swedish company ÅF works as the operating agent of the ICDE project.

The ICDE project allows multiple countries to collaborate and exchange 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 of them to perform meaningful analyses. Input combined from several countries, however, has yielded sufficient data for more rigorous analyses.

Data collection guidelines were developed during the project and are continually revised. They describe the methods and documentation requirements necessary for the development of the ICDE databases and reports. The format for data collection is described in the generic coding guideline and in specific component guidelines. The updated version of the general coding guideline [1] includes modified definitions to the terms “event cause” and “CCF root cause”, the addition of component specific guidelines for main steam isolation valves (MSIV), fans, inverters and digital I&C, and also the failure analysis guideline. The data will be accessible to those participants that have contributed data with a comparable coverage (i.e. covering the same component types and observation periods) through their countries’ national co-ordinators.

Meanwhile, the ICDE project has published reports on the 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 topical reports. This summary report presents recent activities and lessons learnt from the data collection and the results of topical analyses of the ICDE project after phase VII.

The component analysis presents an overview of the entire data set of a specific component type. Topical analyses have been performed for the following topics: external factors [12] (43 events), diesels all affected [13] (143 events), plant modifications [14] (53 events), improving testing [15] (59 events) and multi-unit events [16] (87 multi-unit events). The results in the three latest reports on plant modifications, improving testing and multi-unit events are based on the updated version of the general coding guidelines of ICDE provided during phase VII.

The ICDE data collection provides a structure and basis for component specific quantification of CCF rates and probabilities. A quantitative application example with use of ICDE battery data has been performed. A number of national applications have also been performed based on the ICDE data, e.g. the Nordic C-book [17].

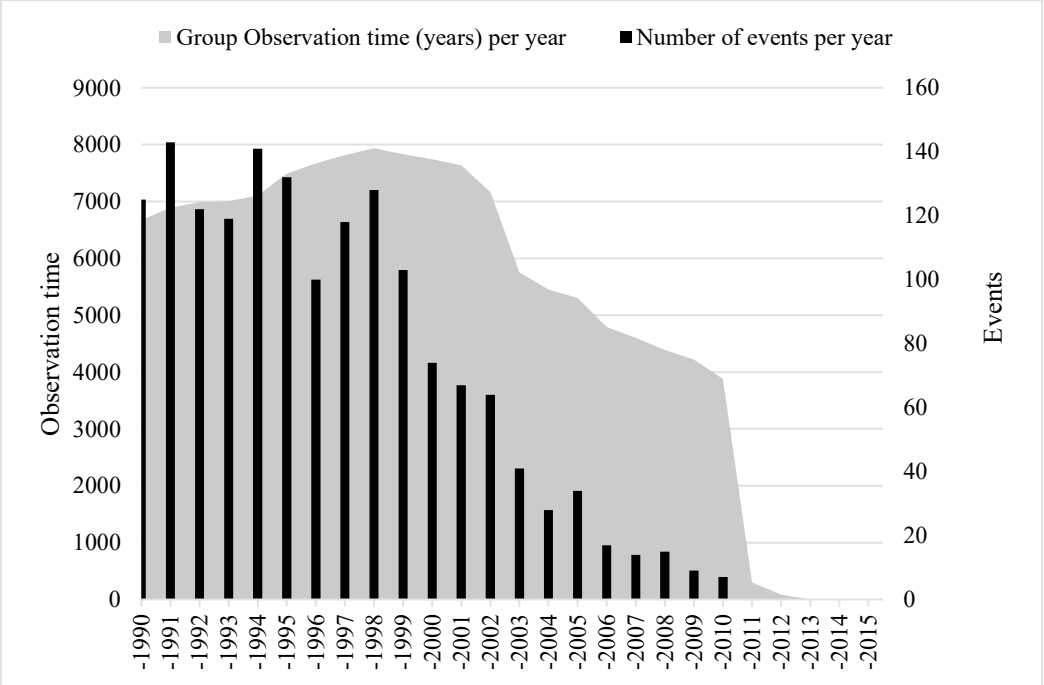
Overall, the ICDE project has well fulfilled its objectives for phase VII (2015–2018), mainly via the topical reports and component reports presented. It should be noted that the ICDE has greatly changed the view of CCFs. For instance, the determination that the most common-cause of complete CCFs seems to be human action as a part of operation (including maintenance and testing) or design, rather than manufacturing deficiencies, would not have been possible without deep plant data collection and combining information from many sources. Perhaps the most important generic lesson is that it is worth forming specialised data exchange projects like the ICDE. This, however, requires the will of several countries to form a critical mass by combining their operating experience efforts. It also requires national efforts to collect and code the data at a more detailed level than those made publicly available as licensee event report (LER) or in International Reporting System for Operating Experience (IRS) reports. Finally, it requires the forming of a legal framework to protect this proprietary data, as well as a long-term commitment to consistently continue and develop the activity.

The NEA, and the ÅF 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.

Challenges and envisaged use for the next project phase are:

- The observed, significant decreasing trend of data submissions to the ICDE project, which underlines the need to improve national efforts to collect and code data on CCF events into the ICDE database. Encouraging participating countries to provide additional CCF data is a great challenge for the ICDE project in future.
- The planned data collection of recently added component types, which will make it possible to identify failure mechanisms, failure causes and possible defences against occurrences of CCF events.
- The relationship of failure mechanism categories and failure cause categories of specific component types, as well as common failure mechanisms across component types, which could be analysed in order to acquire insights into identifying and improving defences against CCF events and decreasing the occurrence of CCF events.
- Topical analyses of intersystem dependencies and pre-initiator human failure events (HFEs), which are ongoing and will provide valuable insights into such events.
- Quantitative application of various component types, which are a possible way to further demonstrate the applicability of the collected ICDE data for quantification.

Figure E1 Observation time and number of events in the ICDE database



List of abbreviations and acronyms

AFWS	Auxiliary feed water system
ANVS	Authority for Nuclear Safety and Radiation Protection (Netherlands)
ASIC	Application specific integrated circuits
ASN	Autorité de Sûreté Nucléaire (Nuclear Safety Authority of France)
BA	Batteries
BWR	Boiling water reactor
CCF	Common-cause failure
CNSC	Canadian Nuclear Safety Commission
CODAP	Component Operational Experience, Degradation and Ageing Programme (NEA)
CP	Centrifugal pumps
CRDA	Control rod and drive assembly
CSN	Consejo de Seguridad Nuclear (Nuclear Safety Council of Spain)
CV	Check valves
CVCS	Chemical volume control system
CSNI	Committee on the Safety of Nuclear Installations (NEA)
DC	Direct current
ECCS	Emergency core cooling system
EDG	Emergency diesel generator
ENSI	Eidgenössische Nuklearsicherheitsinspektorat (Federal Nuclear Safety Inspectorate of Switzerland)
ESFAS	Engineered safety feature actuation system
FIRE	Fire Incidents Records Exchange (NEA joint project)
FPGA	Field programmable gate arrays
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit
HFE	Human failure event
ICDE	International Common-Cause Failure Data Exchange (NEA joint project)
IRS	International Reporting System for Operating Experience (IAEA)
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (Nuclear radiological protection and safety institute of France)
KAERI	Korea Atomic Energy Research Institute
LER	Licensee event report
LM	Level measurement
LOSP	Loss of off-site power
MCC	Motor control centre
MOV	Motor operated valves
MSIV	Main steam isolation valves
MUPSA	Multi-unit probabilistic safety assessment
NEA	Nuclear Energy Agency
NPP	Nuclear power plant
NRA	Nuclear Regulation Authority of Japan
NRC	Nuclear Regulatory Commission (United States)

OA	Operating agent
OECD	Organisation for Economic Co-operation and Development
OP	Observed population
PHWR	Pressurised heavy water reactor
PSA	Probabilistic safety analyses
PWR	Pressurised water reactor
QA	Quality assurance
RPS	Reactor protection system
RTB	Reactor trip breaker
SG	Steering group (also Project Review Group or Management Board)
SRV	Safety and relief valve
SSM	Radiation and Nuclear Safety Authority (Sweden)
STUK	Radiation and Nuclear Safety Authority of Finland
UPS	Uninterruptible power supply/source
WGOE	Working Group on Operating Experience (NEA)

1. Introduction

Common-cause failure (CCF) events can significantly impact the availability of the safety system of a nuclear power plant. In recognition of this, CCF data is systematically being collected and analysed in several countries. Because of the low probability of occurrence of such events, it is not possible to derive a comprehensive evaluation of all relevant CCF-phenomena from the operating experience of 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 nuclear power plant (NPP) operating experience with CCF requires a common understanding of 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 International Common-Cause Failure Data Exchange (ICDE) project.

The ICDE project pursues two main objectives: 1) to collect qualitative and quantitative information about CCFs in NPPs; and 2) to analyse the collected data and distribute the gained insights about CCFs and methods to prevent CCFs in the form of reports to the concerned professional audience. The objectives of the ICDE project as expressed in the agreement are to:

- provide a framework for multinational co-operation;
- collect and analyse 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 defences against the occurrence, such as indicators for risk based inspections;
- generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries;
- use ICDE data to estimate CCF parameters.

1.1. ICDE project organisation

The ICDE project is based upon a broad international co-operation. The central body of the ICDE project is the ICDE steering group (SG) in which each participating country is represented by its national co-ordinator. The SG controls the project, assisted by the Nuclear Energy Agency (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.

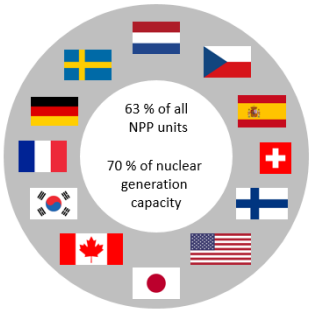
In most countries, the data exchange is carried out through the regulatory bodies, with the possibility to delegate it to other organisations. To ensure that the data collection is performed in a consisted and comparable way in all participating countries the SG has developed and approved "coding guides" 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 to 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 to 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 the NEA and the organisations representing them in the project are: Canada (CNSC), the Czech Republic (ÚJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), Korea (KAERI), the 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.

The countries participating in the ICDE project operate 281 NPP units, which is about 63% of all NPP units worldwide (see Figure 1.1). With a generation capacity of 275 864 megawatts these 281 units provide more than 70% of the worlds' total nuclear generation capacity. The number of 281 units comprises 191 pressurised water reactors (PWR), 68 boiling water reactors (BWR) and 23 pressurised heavy water reactors (PHWR), and so the majority of NPP types is covered.

Figure 1.1 International co-operation and operating experience



The NEA is responsible for administering the project according to OECD rules, which entails overseeing secretarial and administrative services in connection with the funding of the project such as calling for contributions, paying expenses incurred in connection with the OA and keeping the financial accounts of the project. The NEA appoints the project secretariat. To ensure consistency of the data contributed by the national co-ordinators, the project operates through an OA. The OA verifies whether the information provided by the national co-ordinators complies with the ICDE coding guidelines. Jointly with the national co-ordinators, 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 programme: 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).

1.2. Project schedule and resources

Milestones and planning:

The legal agreements are made between the signatories for three-year periods. For this period, a generic project plan is written so that a more detailed plan for every year is presented. The ICDE time schedule defines the milestones of generic data collection tasks. The time schedule is reassessed and revised at each ICDE steering group meeting. The steering group develops future plans. The project status is critically evaluated at each meeting and decisions on how to further proceed are made.

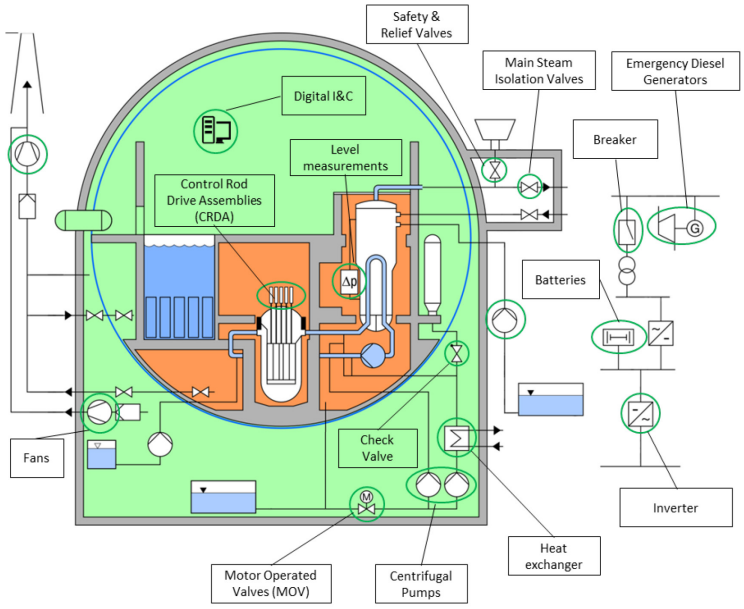
Financial resources:

The NEA prepares together with the OA a general budget frame for the three-year period and specific yearly budgets. All these are subject to SG approval. The NEA makes contracts with the OA for one-year period unless decided otherwise. Participating countries make contributions to a NEA special project account for reimbursement of the costs of the ICDE project OA and NEA Secretariat. In addition, each participant shall carry all other costs associated with the participation in the project.

2. Technical scope of ICDE activities

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 2.1. New component types are added in case there is a corresponding interest of a participating country.

Figure 2.1 Technical scope of ICDE activities



2.1. Component types

An overview of the components types that are covered by the ICDE project are as following.

Centrifugal pumps (CP)

This family of pumps is comprised of those centrifugal pumps (CP) that are motor driven and are used for the purpose of establishing flow to or from the primary system, the secondary system or support systems. This includes, among others the auxiliary/emergency feedwater, high and low pressure safety injection, residual heat removal, essential service water and essential raw cooling water system.

For data evaluation purposes, the family of CP is subdivided into six subgroups characterised by pump delivery head and mass flow rate.

Motor operated valves (MOV)

This family of valves is comprised of those emergency core cooling system (ECCS) valves that are motor operated and are used for the purpose of establishing or isolating flow to or from the primary system, the secondary system or support systems. This includes, among others the auxiliary/emergency feedwater, high and low pressure safety injection, residual heat removal, essential service water and essential raw cooling water system.

Emergency diesel generators (EDG)

EDG are part of the electrical power distribution system providing emergency power in the event of loss of off-site power (LOSP) to electrical buses that supply the safety systems of the reactor plant.

Safety and relief valves (SRV)

The function of the SRV is to prevent overpressure of the components and system piping. The systems respectively components for which SRVs are installed in and data is collected for are the steam generators discharge headers, the pressuriser vapour volume, and the reactor coolant system (main steam headers)

Check valves (CV)

Check valves are used for the purpose of establishing or isolating flow to or from the fluid system. It is comprised of a valve with its internal piece part components. The function of the check valve is to form a conditional boundary (i.e. one direction) between high pressure and low pressure sections of a system during static conditions. By design, the valve will open to allow flow when the low pressure section has experienced a pressure increase (e.g. pump start). This component is operated by system pressure overcoming gravity. Typically, there is no capability to manually open, close or isolate these valves, however, some check valves have manual hand wheels or levers (stop-check) and can be manually closed. Some check valves are “air-testable” which should not affect normal component operation and in some cases the air supply is turned off during operation as a precaution. No power is normally required for valve operation. Check valves are mainly installed in systems in the following areas: pump discharge, pump suction, System inter- or cross-connection, and pump turbine steam inlet.

Batteries (BA)

The family of batteries is comprised of those batteries that provide DC emergency power in the event of a LOSP to DC buses that supply the safety systems of the reactor plant. The voltage to be supplied typically ranges from 24 to 500 V DC.

Level measurement (LM)

The function of the component “level measurement” is to monitor the level in safety relevant vessels, tanks and piping. The output signal of level measurement triggers protection signals in subsequent reactor protection logic system in case of too high or too low level. In ICDE data collection only those level measurement components are considered, which are part of the reactor protection system or part of the engineered safety feature actuation system. Level measurement components which are only used for operational needs (e.g. level control) are not considered.

Switching devices and circuit breakers (BR)

The switching devices and circuit breakers of interest are those that belong to (low/medium voltage) electrical distribution systems (busbar/MCC feeder and load breaker) and reactor trip breakers.

Diesel generator (EDG), motor operated valve (MOV), and motor pump (MP) breakers are included within their equipment boundaries.

The reactor trip breakers (RTBs) are part of the reactor protection system (RPS) of PWR and CANDUs, and supply power to the control rod drive mechanisms. Both AC and DC breakers are used for the RTBs. On a reactor trip signal, the breakers will open, removing power from the control rod drive mechanisms. The control rods will then unlatch and drop into the reactor core due to gravity.

Control rod and drive assembly (CRDA)

The purpose of the CRDA is to control reactivity when the reactor is in normal operating conditions and during rapid transients, and to provide sufficient additional negative reactivity for emergency operating conditions. The consequences related to the failure of the CRDA system depends on the initiator, plant state before scram and the needed effectiveness of the control rod population which is expressed by the minimal number of control rod clusters required at the position in the core cross-section where the control rod clusters failed to insert.

Heat exchanger (HE)

A heat exchanger is a device built for efficient heat transfer from one fluid to another, where the fluids are separated by a solid wall so that they never mix. They are widely used in refrigeration, air conditioning, space heating and power production.

Data is collected for all heat exchangers in safety relevant systems, in particular the heat removal chain (residual heat removal system -> component cooling system -> essential service water).

Fans

The general function of a fan is to ensure the circulation and distribution of air for buildings and rooms (e.g. emergency diesel generator rooms, electrical rooms and electronic equipment rooms). The component operation is running/alternating or standby.

Fan data are being collected for the inlet air, extracted air and recirculating air systems of the safety important buildings. Fans that are within the boundaries of other components (such as motors, pumps or diesels) are not part of the data collection.

Main steam isolation valves (MSIV)

MSIV are fast closing impulse operated valves. The purpose of main steam isolation valves is to isolate the containment or the steam flow to the turbine unit and interfacing auxiliary systems (depending on the plant design). Some plants use separate sets of fast closing impulse operated steam isolation valves with safety relevant functions in the main steam or in the auxiliary steam system for isolation of, e.g. auxiliary steam, main steam relief valves or main steam safety valves. These valves are also covered in this data collection.

Digital instrumentation and control (I&C)

Digital I&C systems are used in different safety related and safety systems of nuclear power plants, such as the RPS, the engineered safety feature actuation system (ESFAS), limitation systems.

They are characterised by the fact that discrete values are used to represent information, e.g. physical parameters. To process the information, they typically comprise computers (which run system and application specific software), microprocessors, microcontrollers, field programmable gate arrays (FPGA) or other complex electronic devices like application specific integrated circuits (ASIC). In many cases, different devices are connected by digital buses.

Inverters

An inverter is a device for converting a direct current into an alternating current. The inverters are used for the purpose of establishing battery backed altering current on safety bus bars. Three different types of inverters can be distinguished: static inverters rotating inverter UPS (uninterruptible power supply/source).

The data collection covers all inverters which are used in safety relevant systems.

2.2. Cross-component group CCF (X-CCF)

A X-CCF event is an event where a single failure mechanism simultaneously affects multiple observed populations (OPs). X-CCF may affect multiple component groups of the same component type as well as different component types. Prominent examples for such CCF events affecting multiple OPs are so-called asymmetrical faults in the on-site power system of NPPs as they have been observed.

Thorough analysis of operational experience from NPPs suggests that there are numerous obvious or hidden dependencies between the individual OPs like common maintenance teams and procedures, piece parts which are used in multiple OPs, shared cooling water, superordinate I&C or internal and external factors which may affect multiple OPs simultaneously.

Even though X-CCF are rare events (only a fraction of all failure events are CCF events and only a fraction of all CCF events are X-CCF events) it is worth to analyse such events in depth since they have the potential to cause severe impairments of the plants safety system.

3. Data collection principles and guidelines

Data collection guidelines have been developed during the project and are continually revised. They describe the methods and documentation requirements necessary for the development of the ICDE databases and reports. The format for data collection is described in the generic coding guideline and in specific component guidelines, see further Section 3.2.

Definition of observed population: set of similar or identical components that are considered to have a potential for failure due to a common-cause. A specific OP contains a fixed number of components. Sets of similar OPs form the statistical basis for calculating common-cause failure rates or probabilities.

Data collection in the ICDE project is based on observed populations which are handled in the database with "observed population records" (or "OP-records") and CCF events which are handled with CCF event records (or ICDE event records). In most cases, the OP-records comprise the redundant, identical components of a system, all performing the same function. Thus, they are equal to the common-cause component groups (CCCGs) explicitly modelled in many probabilistic safety analyses (PSA) such as the parallel pumps in a multi-train safety injection system.

Definition of common-cause events: 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.

3.1. Quality assurance

The data collection and qualitative analysis shall result in quality assured data recorded in databases with consistency verification performed within the project.

The ICDE activity defines the formats for collection of CCF event experience in a quality assured and consistent database. This task includes the development of a set of coding guidelines describing the methods and documentation requirements necessary for the development of the ICDE databases. For more details, see Section 3.2.

The data are collected according to the internal processes of the participating organisations and checked according to their internal quality assurance programmes. The event information provided by the participating organisations is intended to be analysed within the scope of the project; it is not intended that the event data is changed unless the events undergo a review by the responsible national co-ordinator.

The ICDE steering group prepares publicly available reports containing insights and conclusions from the analysis performed whenever major steps of the project have been

completed. The ICDE steering group assists the appointed lead person in reviewing the project report. Otherwise the work follows the quality assurance plans and external review is provided by CSNI/Working Group on Operating Experience (WGOE) and CSNI in sequence.

3.2. General coding guidelines

In the general coding guidelines for the ICDE project, explanations on the ICDE general coding format are given. The guide reflects present experience with the data format and with the collected data. For each component analysed in the ICDE project, separate coding guidance is provided in the appendices, specifying details relevant to the respective components.

Some of the most central coding elements for the ICDE event collection are:

- Failure mode: the failure mode describes the function the components failed to perform.
- Root cause: the most basic reason for a component failure, which, if corrected, could prevent recurrence. The identified root cause may vary depending on the particular defensive strategy adopted against the failure mechanism. In general, the root causes are not based on a formal full scope root cause analysis.
- Coupling factor: the coupling factor describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected.
- Shared cause factor: the shared cause factor allows the analyst to express his degree of confidence about the multiple impairments resulting from the same cause.
- Time factor: this is a measure of the "simultaneity" of multiple impairments. This can be viewed as an indication of the strength-of-coupling in synchronising failure times.
- Corrective action: the corrective action describes the actions taken by the licensee to prevent the CCF event from re-occurring. The defence mechanism selection is based on an assessment of the root cause and/or coupling factor between the impairments.
- Detection method: the detection method describes how the exposed components were detected.
- Component impairment: the impairment expresses the degradation of the individual components. Some or all components are exposed to a common-cause mechanism, but may be affected differently: some may fail completely, some may be degraded, while others remain unaffected. The suffered impairment is described by the component impairment vector. The degradation scale of failure is complete (C), degraded (D), incipient (I) or working (W).

3.3. Component coding guidelines

Component specific guidelines are developed for all analysed component types as the ICDE plans evolve. The ICDE general coding guidelines [1] includes component coding guidelines for centrifugal pumps, motor operated valves, emergency diesel generators,

safety valves/relief valves, check valves, batteries, level measurement, switching devices and circuit breakers, control rod and drive assemblies.

New component coding guidelines planned to be added in the general coding guidelines update (planned 2018) are MSIV, fans, inverters and digital I&C.

For each component type included in ICDE, a component specific coding guideline is developed, defining the component boundaries, event boundary, system types (with corresponding International Reporting System for Operating Experience (IRS) system coding), coding rules and exemptions, functional fault modes, and minimum time periods of exchange.

Component boundary

The component boundary encompasses the set of sub-components or piece parts that are considered to form the component. The component boundary may comprise of different pieces of equipment located in different locations. The component boundaries of the different component types are defined and described in the corresponding component coding guidelines.

Event boundary

The event boundary is component specific and describes the mission of the component. For example, for EDGs it is defined as any condition that does not permit the EDG to start or supply motive force/electrical power in the event of loss of coolant or loss of off-site power. The mission for a centrifugal pump is to maintain the water inventory in the primary system, or to maintain cooling flow in the primary or secondary system or in support systems. Failure of the centrifugal pump to perform its mission occurs if a pump that is required to be running to allow injection or cooling flow fails to start or fails to run.

3.4. Failure analysis guideline

Following the collection of data and ICDE event coding for components, the ICDE steering group initiates and performs the failure analysis assessment. The development of failure analysis provides:

- 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.
- Detailed analyses of failure mechanism sub-categories that will provide valuable insights for improving defences against the occurrence of CCF events.
- Additional aspects when conducting workshops.

The failure analysis elements provide efficient support and transparency to the writing of component or topical reports. 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.

Coding should be done on the available information even if the information in the event description is sparse. However, there should be awareness of that the coding could have been different if more details would have been available. When several consequences are observed in a chain implying that several sub-categories can be assigned to the event, the

first or the most important mechanism should be chosen. The codes are a result of performed work by the ICDE steering group. The technical note update (planned 2018) will include the ICDE failure analysis guideline.

The failure analysis elements are:

- Failure mechanism description: a history describing the observed events and influences leading to a given failure. Elements of the failure mechanism could be a deviation or degradation or a chain of consequences derived from the event description.
- Failure mechanism category and sub-category: component-type-specific observed faults or non-conformities which have led to the ICDE event and a failure mechanism category is a group of similar failure mechanism sub-categories.
- Failure cause category: the codes for failure causes are not component dependent, however, they are dependent on root cause and coupling factor. It is the coupling factor that identifies the mechanism tying together multiple failures and the influences that created the conditions for multiple components to be affected. The root cause alone does not provide the information required for identifying failure cause categories. There are six failure cause categories which are distributed over two types of groups; deficiencies in operation and deficiencies in design, construction and manufacturing.

Severity category classification: the severity classification is an important part in the failure analysis since it correlates the observed event's failure mechanism with a severity degree, i.e. the impact of the failure mechanism. The severity category expresses the degree of severity of the event based on the individual component impairments (C, D, I, W), as described in Section 3.2, in the observed/exposed population. The categories are:

- Complete CCF: all components in the group are completely failed (i.e. all elements in impairment vector are C, Time factor high and shared cause factor high.).
- Partial CCF: at least two components in the group are completely failed (i.e. at least two C in the impairment vector, but not complete CCF. Time factor high and shared cause factor high.).
- CCF Impaired: at least one component in the group is completely failed and others affected (i.e. at least one C and at least one I or one D in the impairment vector, but not partial CCF or complete CCF).
- Complete impairment: all components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components. (all D or I in the impairment vector).
- Incipient impairment: multiple impairments but at least one component working. No complete failure. Incomplete but multiple impairments with no C in the impairment vector.
- Single impairment: the event does not contain multiple impairments. Only one component impaired. No CCF event, but considered interesting by the ICDE data analyst.

4. Insights from data collection and event analysis

Data collection is a continuous process and several event analyses have been performed and published. This chapter presents the status of the data collection, some insights from the specific component analysis and the topical analyses. In addition, failure mechanisms and failure cause are presented for the most severe events, i.e. complete CCFs.

4.1. Data collection overview

An overview of the database content[1] with the number of CCF events and the number of complete[2] and partial[3] CCF events for each component type is given in Table 4.1.

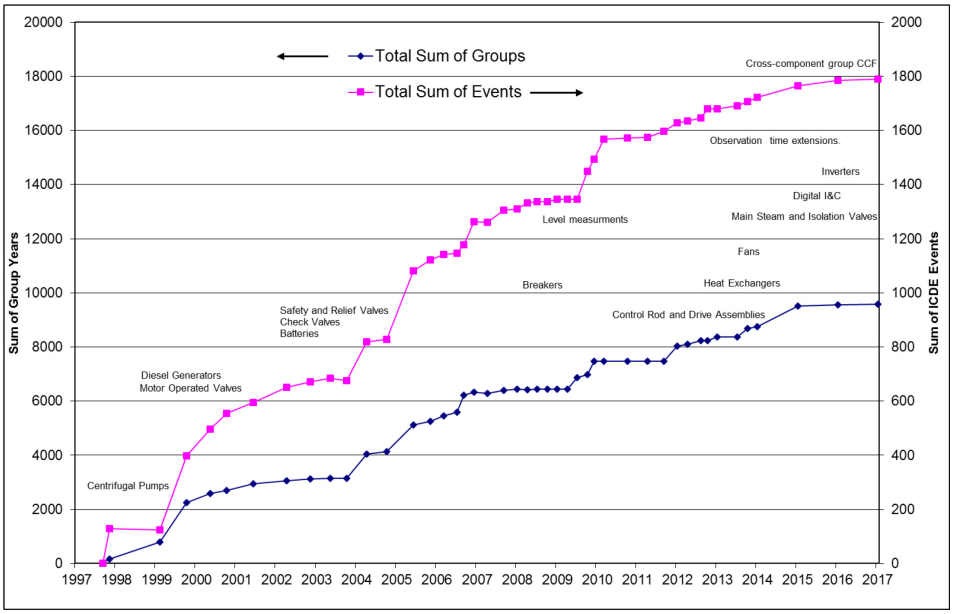
Table 4.1 Data collection overview

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
Digital I&C	4	0.2%	2	0
Cross-component CCF	0	0.0%	0	0
Total	**1 810**	**100%**	**161**	**229**

1. As of 15 November 2017.
2. Complete CCF: a common-cause failure in which all redundant components fail 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”).
3. 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.

The chronological sequence of the data collection is shown in Figure 4.1. The graph shows how new component types were added over time as well as the continuous data collection for the existing component types.

Figure 4.1 Data collection progress in the ICDE database



4.2. Failure mechanisms and failure causes of complete CCF

Events with "complete CCFs" are of particular interest for CCF analysis because they often result in a complete loss of a safety function with a high risk that nuclear safety goals are endangered. Therefore, it is interesting to analyse what factors led to such complete CCFs (i.e. what was the "failure cause") and what can be done to prevent complete CCFs in the safety system of NPPs.

The following observations can be made:

- averaged over all components, almost 60% of all complete CCF events involve human failure, e.g. procedure inadequacy, insufficient maintenance and faulty actions by plant personnel and contractors.

With use of failure mechanism identification and descriptions (see Section 3.4), some exemplary complete CCF ICDE events can be described. The selected events focus on the identified failure mechanisms and failure causes, and include a variety of components.[4]

4. To comply with the ICDE terms and conditions, no plant names, systems codes, dates etc. are included in the event descriptions.

Component type	Failure mechanisms and failure causes
Centrifugal pump	○ Maintenance work on main cooling water pumps led to loss of all reactor coolant water pumps due to changed flow conditions in the common water intake for the pumps during the test. The maintenance procedure had been modified before the event occurred. As corrective action, the procedure was withdrawn and revised once again. ○ Erroneous modifications to the auxiliary feed water system (AFWS) start logic caused all pumps in the component cooling system (CCW) not to start on demand. The event is assessed as a potential intersystem dependency since these systems were sharing the same electrical cubicle. The event would have been prevented by separate sheets of drawings for each system, but it is difficult to defend from this type of events. An improved process for work preparations and better quality assurance (QA) of documentation would also have helped.

Component type	Failure mechanisms and failure causes
Emergency diesel generator	○ Error in the test procedure disabled the automatic start function of all EDGs during test of turbine driven emergency power supply. Knowledge and safety awareness of the personal performing the test led to a fast discovery of the faulty state. Better QA of test procedures would have prevented the event from happening. As lesson learnt, a test may cause problems in another system that is actually tested. ○ Pollution of the air supply due to sandblasting outside the diesel building led to scoring in the sleeves of the cylinders and to high pressure in the motors in two out of two EDGs. An implementation of pressure instrumentation could have prevented the event. Also, verification of operability after maintenance could be improved.
Level measurement	○ Both level transmitters were replaced without updating the calibration procedure which led to the transmitters could not monitor the tank level in the chemical and volume control system (CVCS) correctly. The performed functional test could not detect this fault because the test only could check the level measurement by simulating draining the tank. A functional test with draining of the tank could have prevented the event. ○ The three level transmitters of the pressuriser did not fulfil their function during emergency conditions due to they were not connected to the uninterrupted power supply as designed. During the plant modification, they had been connected to the wrong power supply. A better testing procedure after the plant modification could have prevented the event.

Component type	Failure mechanisms and failure causes
Safety and relief valve	○ Wrong settings for safety relief valves were detected at two groups of valves at a twin-unit site, one in each unit. The reason for the wrong settings were incorrect engineering judgement and identical maintenance actions which were applied for all valves which resulted into a complete CCF (correlation factor; human and organisation) of two groups of safety valves. As defence, it was proposed to introduce a process to ensure completeness, quality and validity of maintenance procedures e.g. by an independent verification of the used input data and calculations.
Motor operated valves	○ Design modifications at the logic of the containment isolations were erroneously not applied for a group of motor operated valves in the residual heat removal system. Because of this, containment isolation would not have been available for the plant shut down phase as required in the technical specifications. The design should have been reviewed and tested for all plant modes, and the testing of the modification during plant shutdown should have been performed. Diverse maintenance teams would increase the possibility to identify such failures.

4.3. Component analysis

A component analysis presents an overview of the entire data set of a specific component type. The data are not necessarily complete for each country but all available approved data is used. The overview includes information about the event parameters root cause, coupling factor, observed population (OP) size, corrective action, the degree of failure, affected subsystem and detection method. The degree of failures is based on defined severity categories, which are used in the assessment. Charts and tables are provided exhibiting the event count for each of these event parameters.

The component analysis also includes analysis of engineering aspects of the events, which presents a qualitative assessment of the collected data. Events are analysed with respect to failure mechanisms and failure cause categories through use of an assessment matrix.

The objectives of the component analysis are:

- to describe the data profile for component type in question;
- to develop qualitative insights in the nature of the reported events, expressed by root causes, coupling factors, and corrective actions; and
- to develop the failure mechanisms and phenomena involved in the events, their relationship to the root causes, and possibilities for improvement.

Public final reports for centrifugal pumps, diesel generators, motor operated valves, safety and 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]-[11]. In total, 1 421 ICDE events have been analysed in the component reports.

4.3.1. Data profile

The data profile presents an overview of the collected component's data set, including the event count and the total observation period, see Figure 4.2. and Figure 4.3. The events are examined by tabulating the data and observing trends. Once trends are identified, individual events are reviewed for insights. For example, the updated diesel report [3] includes 224 CCF events spanning a period from 1977 through 2012.

Figure 4.2 Observation time and number of events in the ICDE database

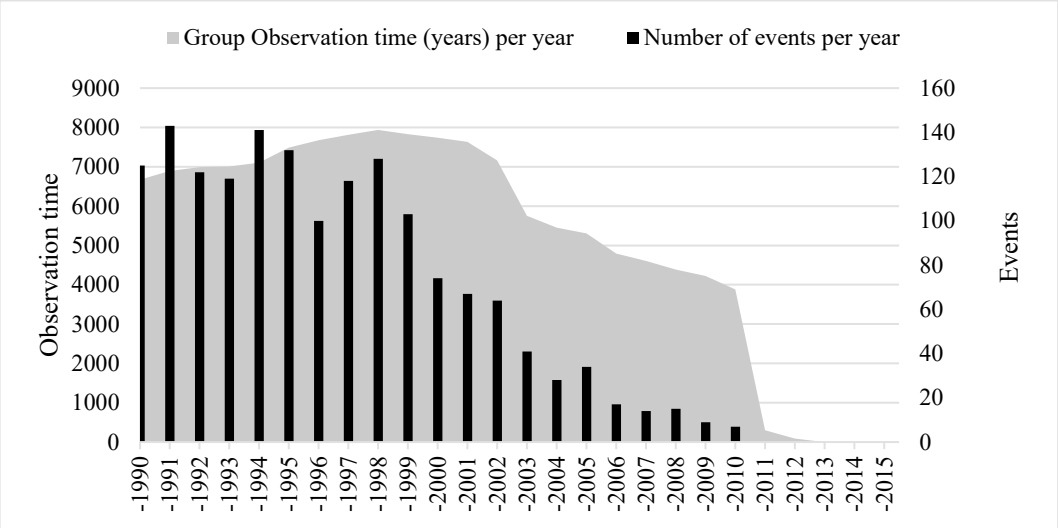
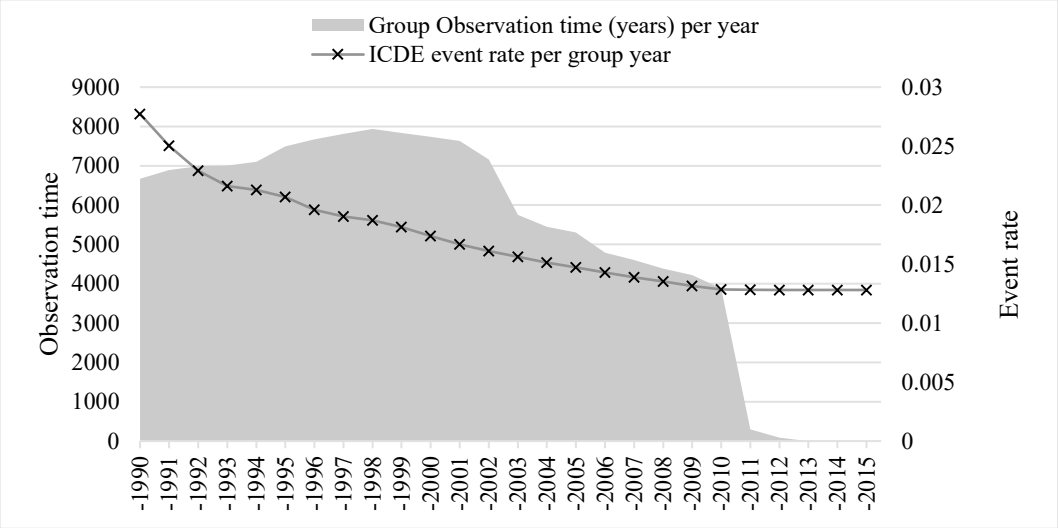


Figure 4.3 ICDE data event rate



4.3.2. Failure mechanism categories and failure phenomena

Failure mechanisms categories are defined in an iterative process based on the observed events. The final list of categories can also be looked upon as a summary description of the event observation. Examples of concluded failure mechanism categories from the updated diesel report are:

- engine damage or problems, such as:
  - starting air or air supply valve/distributor damage, 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 damage (between engine and generator), combustion/charging air problems (e.g. air intake, turbocharger damage);
- compromised ancillary systems, such as:
  - cooling water (missing or low water pressure, temperature, leakage), lubrication (missing lube oil or low lube oil pressure, bad quality, or wrong temperature of lube oil), compromised air intake or cooling of ventilation, fuel (quantity, quality, leakage);
- electrical failures, such as:
  - alternator damage, breaker/relay failure, other electrical damage (e.g. of cables, cabinets);
- Deficient control and deficient protective cut-out (I&C problems), such as:
  - defective or unsuited piece part, misadjusted set points, inadvertent actuation of protective cut-out or fire protection system;
- misalignment, such as:
  - faulty sub-component, faulty system configuration/operator control actions, faulty logic.

4.3.3. Qualitative insights

The component analysis is finally concluded into insights and lessons learnt, based on the data review and observed failure mechanisms. Example of such observation are taken from the updated diesel report. The following notable observations were made:

- The most frequently occurring causes of emergency diesel generator failures are design errors related to design, manufacture or construction inadequacy.
- Events with failure causes related to deficiencies in operation tend to include a higher proportion of severe failures.
- Maintenance/test was the main way of detecting problems with the diesels, followed by unknown detection methods and test during operation. The share of demand events is low compared with other components.
- The most common diesel generator failure mechanism category is comprised ancillary systems, with many failures involving cooling water or fuel supply systems.
- I&C failures are more likely than other types of failure mechanisms to result in severe CCF events that completely fail multiple components in a group.
- 10% of the reported ICDE diesel generator events are complete CCF events. This is the most severe failure category with complete failure of all diesels in the common-cause component group.
- 50 diesel generator CCF events have been marked as impacting multiple reactor units.

4.4. Topical analysis

The ICDE steering group has developed a work procedure for topical analysis, which supports the analysis of events. The work procedure includes the failure analysis elements (as presented in Section 3.4). The procedure aims to capture insights for possible improvements and defences for the topic in question. The defences try to identify aspects that prevented the event from developing into a complete CCF. The improvements identify areas that could be improved to prevent the event from happening again. Topical analyses have been performed for the following topics:

- external factors [12] (43 events);
- diesels all affected [13] (143 events);
- plant modifications [14] (53 events);
- improving testing [15] (59 events);
- multi-unit events [16] (87 multi-unit events).

For the topical analyses, the findings and conclusions are presented in the following sections.

4.4.1. CCFs due to external factors

In the light of the Fukushima Daiichi accident, a cross-component study was performed on a set of common-cause failure events due to external factors, which includes “external

events" and other external environmental factors that can impact plant operation. This means that the scope of the "external factor" topic included not only storms, hurricanes and severe weather events, but also other environmental conditions, such as, high outdoor temperatures and excessive algae growth. The external factor study included analysis of 43 external factor events, 19 events were caused by extreme weather conditions and 24 events were caused by physical phenomena unrelated to weather conditions, for example clogging by sand or algae or other pollution effects and earthquake. This topical analysis is complete and the report has been published [12]. Representative failure mechanisms sorted by component type are:

Component type	**Occurred failure mechanisms**
– Battery	o potential loss of function during earthquake due to cracks in battery casings.
– Centrifugal pump	o freezing led to blocking by ice of suction lines of service water pumps; o heavy seaweed accumulation in combination with low tide caused lack of water; o excessive sand and shellfish in sea water led to wear of pump impeller; o sandy water intrusion and corrosion products lead to clogging of bearing lube water lines; o extremely low level of sea water was not considered in design; o algae growth in diesel fuel tank led to failure of operation of diesel driven pumps;
– Diesel	o sludge in sea water reduced cooling capacity; o excessive sand and shellfish in sea water led to clogging of heat exchangers.
– Heat exchanger	o high temperatures led to fast growth of clams and mussels with subsequent clogging of heat exchangers; o very high water level in combination with highly polluted water (foliage and grass) led to clogging of heat exchangers.
– Safety and Relief Valve	o diaphragms installed in the air supply regulators of safety relief valves were dry and cracked due to long-term high temperature environment leading to failure to open of the valves.

Human and operational related improvements

"Increased monitoring" was one of the most common type of operational improvements which was concluded for events involving pumps, diesels and heat exchangers. "Increased monitoring" involves more frequent monitoring or more efficient monitoring techniques. Surveillance procedure was identified to be a successful defence. Three events involved slow processes where excessive sand or shellfish in the sea water caused wear of the pump's impeller or clogging in the heat exchanger. Due to the slowly developing failure, it was possible to detect the events before developing into complete failures.

Also "improved cleaning of strainers" was concluded as an important improvement for events involving pumps, diesels and heat exchangers, with the majority representing heat exchanger events. All five heat exchanger events involved high sea water temperatures leading to fast growth of clams and mussels and simultaneously clogging of the heat exchangers. Improved procedures were identified to be important, along with enhanced monitoring capability.

Three diesel events within three years at the same site experienced the same failure mechanism are proof that back fitting of operational experience takes long time. These events involved sludge in the sea water leading to reduced cooling capacity and therefore to too high temperatures of the diesel´s cooling water. Here it could be concluded that thorough root cause identification before continuation of operation is crucial to prevent repetitions of the failure.

Hardware related improvements

Since many of the events due to external factors involve sea water problems, important hardware improvements involve design changes of the water intake. One pump event revealed that there had been insufficient attention to possible low level of sea water. The same diesel event mentioned above (work event D2), where sludge in the sea water led to reduced cooling capacity and therefore to too high temperatures of the diesel's cooling water, could have been prevented if the water intake had been diversified. An example of a diversified water intake could be one surface intake and one deep water intake. Another interesting event was a pump event where both emergency feed water pumps driven by diesel engines were degraded due to algae growth in the shared diesel fuel tank. The shared fuel tank is an example of not consequently implemented separation of redundant pumps.

The results of this analysis may serve as input for an in depth review of the methods and assumptions used in external hazards PSA.

4.4.2. Diesels affecting entire exposed population

The scope of "diesels all affected" topic was to identify failure mechanisms that are able to impact all diesels in an exposed population, so-called "all affected" diesel failures (in total of 142 events). "All affected" diesel failures involve events where all diesels in an exposed population either failed or were degraded or showed an incipient impairment due the same cause. The scope aimed to get broader insights in failure mechanisms that are potentially able to lead to complete common-cause failures of emergency diesel generators. This topical analysis is complete and the report has been published [13]. One part of the analysis is to try to identify areas of improvement to prevent the event for happening again with use of so-called "improvement categories". An event can be assigned to multiple categories.

a. design of system or site;

b. design of component;

c. surveillance of component;

d. maintenance or testing of component;

e. operation of component;

f. management system of plant.[5]

The most commonly assigned category was "maintenance or testing of component" (34%). Many of these events involve improper re-installations or re-assemblies after testing/maintenance. Suitable prevention of this kind of failure would mean improved test/maintenance procedures, which would include checks after completion of test/maintenance. Approximately 15% of the events were concluded with this type of prevention. 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 events (16%) that were assigned to "management system of plant", improved QA of the vendor was pointed out several times. Evidence was found of that "QA of vendor" not only involves quality assurance of the actual product but also that the product information delivered together with the product must be sufficient.

For the category "design of system or site", 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 was observed.

In the category "surveillance of component", blockage in heat exchanger tubes (primarily corrosion) 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 the diesel fuel supply can be an appropriate improvement.

An example in the category "operation of component", was an event where high iron content of well-water led to dirt deposition on the heat exchanger and too high temperature of diesel engine. One lesson learnt from this event is that controlling the water chemistry of the cooling water is important.

4.4.3. CCFs due to plant modifications

The topical analysis report *"CCFs due to plant modifications*" evaluates CCF events that occurred due to modifications, back fitting, and/or replacements. However, there were no CCF events identified that were related to modifications resulting from a regulatory back fit, i.e. relating to new or amended regulatory requirements or regulations.

The share of complete CCFs (22%) of all modification CCFs was significantly larger than the share of complete CCFs (about 10%) of all CCFs in the database. A time-separated implementation of modifications of modified components could reduce the possibility of all components to be affected by an unanticipated erroneous modification.

For the severe events (complete or partial CCF), I&C modifications were most common. Several problems relate to modified protection devices of the main components (e.g. protection relays, contacts and wiring). This finding also underlines the importance of

5. QA of vendor, spare parts management, training of personnel, sufficient resources/staff, etc.

a complete and thorough system evaluation including a full-featured test programme after modifications.

The following generic insights and recommendations can be given regarding the question on how to prevent CCF events due to modifications:

- Modifications to the safety systems of a nuclear power plant (NPP) have the potential to cause CCFs, especially CCFs that affect all redundant components at once.
- A stringent, comprehensive planning of the intended modifications should be performed, including the assessment of possible interactions on system-level.
- A comprehensive post-modification testing programme should be developed and implemented.
- Modifications of settings, testing procedures and maintenance procedures (e.g. change of lubrication, grease etc.) should be comprehensively tested after the modification.
- If possible, modifications in redundant trains should not be implemented simultaneously to increase the chance that problems are identified by testing.
- Modifications to I&C systems and protection devices should be performed with special care.
- CCFs due to the modification of sub-components are mostly related to the design of the sub-component itself and can be prevented by the owner by a thorough design evaluation and a profound review of the manufacturers.

It shall be noted that in some ICDE events the above mentioned protective measures prevented all components to fail and a complete CCF event did not occur. For other ICDE events, the failures were slowly developing over time and detected, e.g. during periodic testing, before developing into complete CCFs.

4.4.4. Provision against CCFs by improving testing

The main objective of the topical report *"provision against CCFs by improving testing"* was to study CCF events, where 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 report is mainly intended for designers, operators and regulators to enlarge their understanding on reducing CCF risks by improving testing and to give insights of relevant failure mechanisms.

It summarises the results of two data analysis workshops performed by the ICDE steering group, and presents CCF defence aspects for provision against CCFs by improving testing. The event set included 59 improving testing events. In addition, seven events were assessed as plant commissioning error events which were treated separately.

The analysis included an assessment of the event parameters; event cause, coupling factor, detection method, corrective action and event severity. The following noteworthy observations can be made.

- The most common component types were emergency diesel generators, centrifugal pumps and safety relief valves. Level measurements contribute with several severe events.

- The most common CCF root cause was procedure deficiencies (58%).
- Inadequacies in testing have been observed in all investigated aspects of testing, which are: *extent of test, QA of test, performing the test and verification of operability.*
- The most common area to find test inadequacies is in QA of testing.
- No event was identified to be caused by inadequate test intervals.

The most common areas of improvement were testing procedure, maintenance procedure and management of plant.

The lessons learnt from the engineering aspects analysis of improving testing events are:

- A process for QA 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 strong safety culture to prevent deviations from procedures especially in the verification of the work performed.
- 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 events from becoming complete CCFs shows that experience feedback from other units and previous similar events can be a successful way to detect latent failures in time, even when ordinary testing does not identify the failure mechanism.

4.4.5. Multi-unit CCF events

The main objective of the topical report "multi-unit CCF events" was to study CCF events that occurred at multiple units at the same site. The report is mainly intended for designers, operators and regulators to improve their understanding on multi-unit CCF events and to give insights of relevant failure mechanisms.

The observed multi-unit events were classified as: internal factors (shared design or organisational factor), external factors (physical, external or environmental connection), or fleet CCF events (same or similar events occurring at multiple sites). The analysis included an assessment of the event parameters; event cause, coupling factor, detection method, corrective action, CCF root cause and multi-unit event severity. The following noteworthy observations can be made.

- Multi-unit events were observed for a wide range of component types. Emergency diesel generators and centrifugal pumps accounted for more than 50% of the events.
- The most common CCF root cause (nearly 60%) for multi-unit CCF events was deficiency in the design of components and systems. Hence design is significantly overrepresented compared to the total observed CCF event population.
- Events with observed environmental deficiencies were caused by harsh environmental conditions, such as severe weather or abnormal debris in a raw water source which usually require design improvements to prevent reoccurrence.

- About 10% of the events were complete multi-unit CCF events.

The conclusion from the engineering aspects of the multi-unit CCF events were:

- A total of 57 events were dependent through internal factors, where 27 of these events were correlated to "identical design" (for example, same design of components/systems, operating environment or installation) and 17 were correlated by "organisational aspects" (mainly by test and maintenance procedures).
- Feasible defence strategies for the internal multi-unit CCF events 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. Also, some failures were slowly developing in time and could be detected before developing into complete CCFs.
- A total of 14 events were dependent through external factors, where ten of these events were correlated to "shared structures, systems and components (SSCs)" (for example, units with shared water intake channel). Four of the nine complete CCFs were caused due to shared SSCs.
- Feasible defence strategies for the external multi-unit CCF events are "design of system or site" such as better design of water intake; add back-flushing capability, cleaning of strainers etc. Also, improved surveillance/maintenance is a feasible defence to detect the problems before the components fail.
- The multi-unit CCF events identified can provide useful insights to inform multi-unit probabilistic safety assessment (MUPSA) modelling. The external factor events can provide insights relevant to the modelling of physical connections and dependencies across unit boundaries. The internal factor events can provide insights relevant to the need for defining new CCF groups by combining common-cause component groups across units at the site.

5. Envisaged use and further development of ICDE

The ICDE project has changed the view of CCFs a great deal. For instance, the determination 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 extensive plant data collection and combining information from many sources.

Perhaps the most important generic lesson is that it is worth forming specialised data exchange projects like ICDE. 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 component operational experience, degradation and ageing programme (CODAP) for pipe failure events and the fire incidents records exchange project (FIRE) for NPP fire events.

Overall, the ICDE project has quite well fulfilled its objectives for phase VII (2015–2018). In the following sections, the methods of fulfilling these qualitative and quantitative objectives are presented.

5.1. Data collection and coding guidelines

Data collection and data exchange for "standard" component types continue as a part of the general ICDE operation.

The data collection of "new" component types (digital I&C, inverters, cross-component group CCF events) has just begun. The planned data collection of these components will make it possible to identify failure mechanisms, failure causes and possible defences against occurrences of CCF events.

The data collection, as seen in Section 4.1 and 4.3.1, shows a significant decreasing trend of data submissions to the ICDE project, which underlines the need to improve national efforts to collect and code data on CCF events into the ICDE database. This will be one of the challenges in the next project phase.

Coding guidelines

The general coding guidelines for ICDE are presented with explanations and appendices for each analysed component. The guide reflects the present experience with the already completed data collection. New component types are added in case there is a corresponding interest of a participating country. As data collection continues, new needs and interests may arise for further development of the ICDE guidelines.

A part of the general coding guideline is the failure analysis. The failure analysis is performed by the ICDE project participants during dedicated workshop sessions. The failure analysis assessment allows the ICDE participants to perform an in-depth review of the event data from all the participating countries. This failure analysis approach helps the ICDE group develop common insights and trends across the entire data population. These

evaluations have revealed insights that would otherwise not have become evident. The failure analysis codes are a result of work performed by the ICDE steering group, and further analysis will lead to more insights about the collected data. The ICDE is currently preparing the following report [1]:

Technical Note on the ICDE Project General Coding Guidelines (Update and extension of NEA/CSNI/R(2011)12 – NEA/CSNI/R(2004)4)

5.2. Qualitative analysis

Failure analysis presentation

A list of the failure mechanism descriptions can be an easy, yet efficient, way to summarise the type of failures for a certain scope of events. A central part of the specific component type report is the presentation of the relationship of failure mechanism categories and failure cause categories (matrices with failure mechanism categories and failure cause categories). They could provide valuable insights for improving defences against the occurrence of CCF events.

Component and topical analysis

As presented in Section 4.3 and 4.4, the ICDE project has several parallel analyses ongoing. The qualitative analyses will continue and result in insights and lessons learnt about the collected data. This work is part of one of the objectives of the ICDE project phase VII, to generate qualitative insights of CCF events for their prevention or for mitigation of their consequences.

Reports in preparation [14-16] include:

- ICDE topical report: collection and analysis of common-cause failures due to plant modifications;
- ICDE topical report: provision against common-cause failures by improving testing;
- ICDE topical report: collection and analysis of multi-unit common-cause failure events.

Future component and topical analysis

Topical analyses in its initial phase are:

- intersystem dependencies;
- pre-initiator human failure events (HFEs).

Other interesting topics that are being discussed are safety culture and grease/lubrication issues.

In general, component specific insights would be derived, but for several failure mechanism categories/sub-categories cross-component type insights could also be obtained if failure mechanism categories/sub-categories are common to several components.

Problems with lubricants are predominantly caused by errors in operation, mainly deficient maintenance procedures and too long maintenance intervals. By improving maintenance procedures and reducing maintenance intervals the occurrence rate of such events could be significantly reduced. More detailed analyses could provide recommendations for maintenance intervals and procedures to be applied to piece parts and used lubricants that

are identified to be critical by the collected data on failure mechanism sub-categories. An important parameter to be considered in this context would be the degree of impairment associated with the events.

Other failure mechanism sub-categories to be examined in detail could be, for example:

- bearing problems in diesels and centrifugal pumps;
- degraded or broken moving parts in diesels and centrifugal pumps;
- wrong set points in all types of valves, breakers, level measurement devices;
- misadjusted seat/disc configurations in all types of valves;
- broken, bent or otherwise degraded mechanical parts in all types of valves and breakers.

This cross-component type of failure analysis can improve the search for CCF defences and decrease the occurrence of CCF events.

5.3. Quantitative analysis

The general frequency of observing an ICDE event in an observed population (CCF component group) is approximately 0.015/year (or <2E-6/h). The ICDE data collection provides a structure and basis for component specific quantification of CCF rates and probabilities. However, several precautions must be respected to avoid over or under estimation. The precautions to consider are:

- Completeness of CCF event set and observation periods: answers whether the provided set of CCF events covers the whole available national CCF experience, and answers whether group year observation estimate in relation to reported event data set is correct.
- Event interpretation with respect to PSA failure combinations: depending on the used CCF-model, a transformation of the data, for example, into an "event impact vector" is necessary for quantitative CCF parameter estimation.
- Applicability of CCF events: to achieve quality assurance of the data input to the analyses, the events shall be analysed and reviewed in a team review. Individual specific assessment is necessary to decide whether to take the event into account or not.
- Applicability of observed populations: component groups and events shall be divided and grouped to ensure that the quantification is made on a homogenous set of data. This means that the data set should be divided based on homogeneity issues, but only to such extent that the data sets do not become to scarce.
- Parameter estimation methodology: different methods for parameter estimations are used today for quantitative CCF parameter estimation. Independent of choice of methods, several characteristics needs to be considered and some feature of the method may have high impact on the CCF parameter estimation results.

A quantitative application example with use of ICDE battery data has been performed. This application demonstrates the use of ICDE database and examines the applicability of the ICDE data for quantification. Additional application examples of other component types are a possible way to further demonstrate the applicability of the collected ICDE data for

quantification. A number of national applications have also been performed based on the ICDE data, e.g. the "Nordic C-book" [17].

5.4. More information

More information about ICDE project may be obtained by visiting:

- The NEA website: www.oecd-nea.org/jointproj/icde.html;
- The CSNI report webpage: www.oecd-nea.org/nsd/docs/indexcsni.html;
- Operating agent website: https://projectportal.afconsult.com/ProjectPortal/icde.

or by contacting the responsible NEA project administrator.

6. References

List of Publications:[6]

1. Technical Note on the ICDE Project General Coding Guidelines. (Update and extension of NEA/CSNI/R(2011)12 – NEA/CSNI/R(2004)4), September 2018
2. NEA/CSNI/R(2013)2 ICDE Project Report: Collection and analysis of common-cause failure of centrifugal pumps. (Update of NEA/CSNI/R(99)2)
3. NEA/CSNI/R(2018)5 Lessons Learnt from Common-Cause Failure of Emergency Diesel Generators in Nuclear Power Plants – A Report from the International Common-Cause Failure Data Exchange (ICDE) Project. (Update of NEA/CSNI/R(2000)20)
4. NEA/CSNI/R(2001)10 ICDE Project Report on Collection and Analysis of Common-Cause Failures of Motor Operated Valves.
5. NEA/CSNI/R(2002)19 ICDE Report on Collection and Analysis on Safety and Relief Valves.
6. NEA/CSNI/R(2003)15 ICDE Project Report on Collection and Analysis of Common-Cause Failures of Check Valves.
7. NEA/CSNI/R(2003)19 ICDE Project Report on Collection and Analysis of Common-Cause Failures of Batteries.
8. NEA/CSNI/R(2008)1 ICDE Project report: Collection and analysis of Common-cause Failures of Switching Devices and Circuit Breakers.
9. NEA/CSNI/R(2008)8 ICDE Project Report: Collection and Analysis of Common-Cause Failures of Level Measurement Components.
10. NEA/CSNI/R(2013)4 ICDE Project Report: Collection and analysis of common-cause failure of control rod drive assemblies.
11. NEA/CSNI/R(2015)11 ICDE Project Report: Collection and analysis of common-cause failure of heat exchangers.
12. NEA/CSNI/R(2015)17 ICDE Project Report: Workshop on Collection and Analysis of Common-Cause Failures due to External Factors
13. NEA/CSNI/R(2017)8 ICDE Workshop - Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Population.
14. NEA/CSNI/R(2019)4 ICDE Project report: Collection and Analysis of Common-Cause Failures due to Plant Modifications

6. Reports may be downloaded from the NEA website at: www.oecd-nea.org/nsd/docs/indexcsni.html

15. NEA/CSNI/R(2019)5 ICDE Project report: Provision against Common-Cause Failures by Improving Testing
16. NEA/CSNI/R(2019)6 ICDE Project report: Collection and Analysis of Multi-Unit Common-Cause Failure Events

Other references:
17. Nordic C-book. Håkansson, M, Johanson, G. (2017). C-book CCF Reliability Data Book Part 1. NPSAG Report 44-002:01. http://npsag.org/publications/