Nuclear Energy Agency

NEA/CSNI/R(2020)1

Unclassified English text only

23 May 2022

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

ICDE Topical report: Collection and Analysis of Intersystem Common-Cause Failure Events

This document is available in PDF format only.

JT03495921

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) is responsible for the Nuclear Energy Agency (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.

Foreword

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. In 1997, the Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) formally approved carrying out this project within the NEA framework; since then the project has successfully operated over seven consecutive terms (the current eighth term covering the period 2019-2022).

The purpose of the ICDE project is to allow multiple countries to collaborate and exchange 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, yield sufficient data for more rigorous analyses.

The objectives of the ICDE project are to:

- collect and analyse CCF events over the long term to better understand such events, their causes, and their prevention;
- generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or to mitigate their consequences;
- establish a mechanism for the efficient feedback of experience gained in connection with CCF-phenomena, including the development of defences against their 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 the ICDE data to estimate CCF parameters.

The qualitative insights gained from the analysis of CCF events are made available by reports that are distributed without restrictions. It is not the aim of those reports to provide direct access to the CCF raw data recorded in the ICDE database. The confidentiality of the data is a prerequisite of operating the project. The ICDE database is accessible only to those members of the ICDE project working group who have contributed data to the databank.

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 produced the following reports, which can be accessed through the NEA website:

- Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(99)2], September 1999.
- Collection and analysis of common-cause failure of emergency diesel generators [NEA/CSNI/R(2000)20], May 2000.
- Collection and analysis of common-cause failure of motor-operated valves [NEA/CSNI/R(2001)10], February 2001.
- Collection and analysis of common-cause failure of safety valves and relief valves [NEA/CSNI/R(2002)19], October 2002.
- Proceedings of ICDE Workshop on the qualitative and quantitative use of ICDE Data [NEA/CSNI/R(2001)8, November 2002.
- Collection and analysis of common-cause failure of check valves [NEA/CSNI/R(2003)15], February 2003.
- Collection and analysis of common-cause failure of batteries [NEA/CSNI/R(2003)19], September 2003.
- Collection and analysis of common-cause failure of switching devices and circuit breakers [NEA/CSNI/R(2008)01], October 2007.
- Collection and analysis of common-cause failure of level measurement components [NEA/CSNI/R(2008)8, July 2008.
- Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(2013)2], June 2013.
- Collection and analysis of common-cause failure of control rod drive assemblies [NEA/CSNI/R(2013)4], June 2013.
- Collection and analysis of common-cause failure of heat exchangers [NEA/CSNI/R(2015)11], April 2013.
- ICDE Workshop – Collection and Analysis of Common-Cause Failures due to External Factors [NEA/CSNI/R(2015)17], October 2015.
- ICDE Workshop – Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Population [NEA/CSNI/R(2017)8], August 2017.
- 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 [NEA/CSNI/R(2018)5], September 2018.
- ICDE Project Report: Summary of Phase VII of the International Common-Cause Data Exchange Project NEA/CSNI/R(2019)3, June 2019.
- ICDE Topical report: Collection and Analysis of Common-Cause Failures due to Plant Modifications NEA/CSNI/R(2019)4, 2019.

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

Acknowledgements

The following individuals have significantly contributed to the preparation of this report by their personal effort: Gunnar Johanson (ÅF), Mattias Håkansson (ÅF), Benjamin Brück (GRS) and Jeffery Wood (NRC).

In addition, the ICDE working group and the people with whom they liaise in all participating countries are recognised as important contributors to the success of this study. Olli Nevander and Diego Escrig Forano have successively served as the administrative NEA officer and contributed to finalising the report.

Table of contents

Tables

Figures

Executive summary

This report presents a study performed on a set of common-cause failure (CCF) events within the International Common-Cause Failure Data Exchange (ICDE) project. The topic of the study was intersystem dependencies, i.e. events from the operating experience with nuclear power plants where a single CCF mechanism affected components in multiple different systems of the nuclear power plant.

The report also addresses the occurrence of multiple CCF events in only one system with no indications that other systems might also have been affected. These are not ordinarily considered intersystem events but are included in this report as they are considered interesting events since they involve dependencies between CCF groups which are not specifically modelled in a probabilistic risk assessment (PRA).

The report is mainly intended for designers, operators and regulators to provide insights into the rare intersystem events in the ICDE database. The insights can give valuable experience to support and improve the modelling of intersystem dependencies in the PRA models and provide intersystem CCF data for quantification purposes.

The report summarises the results of a data analysis workshop performed by the ICDE steering group, presents CCF defence aspects for intersystem CCF events, and includes in total 25 events. The analysis included an assessment of the event parameters, event cause, coupling factor, detection method, corrective action, and event severity. The most noteworthy observation was that the most common CCF root cause was "solely or predominantly design" (72%). However, for the more severe events, the dominant CCF root cause was procedure deficiency.

The analysed events show evidence of internal and external intersystem CCF events, and also inter-CCF group events. Thus, intersystem dependencies need to be addressed for all types of potential system dependencies. The lessons learnt from the engineering aspects analysis of the intersystem CCF events and the resulting recommendations are:

- Intersystem CCFs are rare events (the 25 events correspond to about 1.4% of all CCF events in the ICDE database and about 1.9% of the complete CCFs, i.e. ~0.02 in an intersystem β-factor model), yet their existence and their risk significance should not be overlooked.
- The observed intersystem dependency events cover a wide range of component types, systems and failure mechanisms. Thus, there are no component types which are especially vulnerable or robust against intersystem CCFs, i.e. no particular trend can be observed in the data.
- Highly redundant component types, such as safety and relief valves (SRV) and control rods and drive assemblies (CRDA), were not observed among the events (these components are not intersystem systems by design).
- Modification of component protection devices (overcurrent, torque, etc.) should be performed with great care. If possible, only one system redundancy

should be modified until sufficient operating experience is gathered to ensure its adequacy.

- Maintenance or modification activities in one system resulting in a CCF in another system were observed. Sharp attention should be paid when planning maintenance or modification activities to ensure that the activities do not affect other systems.
- Diversity on the component level does not ensure diversity on piece part level in different systems. For example, the same type of breaker is used in multiple systems and is vulnerable to a CCF mechanism.
- Thus, intersystem dependencies could exist on a lower component level which is normally not considered in a PRA. Due to its risk significance, intersystem dependencies should be taken into account accordingly when performing a PRA, while also considering the rarity of these events and credit for defences that could prevent or mitigate their occurrence.

List of abbreviation and acronyms

AFWS	Auxiliary feed water system
ANVS	Autoriteit Nucleaire Veiligheid en Stralingsbescherming (Netherlands)
CCCG	Common-cause component group
CCF	Common-cause failure
CCI	Common-cause initiator
CCWS	Component cooling water system
CNSC	Canadian Nuclear Safety Commission (Canada)
CSNI	Committee on the Safety of Nuclear Installations
EDG	Emergency diesel generator
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat (Switzerland)
ESWS	Essential service water system
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
ICDE	International common-cause failure data exchange
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (France)
MOV	Motor operated valves
NEA	Nuclear Energy Agency
NRA	Nuclear Regulatory Authority (Japan)
NRC	Nuclear Regulatory Commission (United States)
OECD	Organisation for Economic Co-operation and Development
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
QA	Quality assurance
SSM	Swedish Radiation Safety Authority (Sweden)
SRV	Safety and relief valves
STUK	Finnish Centre for Radiation and Nuclear Safety (Finland)
TSO	Technical support organisation
UJV	Nuclear Research Institute (Czech Republic)

Note: The acronyms from the ICDE general coding guideline (NEA, 2019) are presented in Annex C.

1. Introduction

The main objective of the International Common-Cause Failure Data Exchange (ICDE) project is to generate qualitative insights regarding the causes of common-cause failure (CCF) events that can be used to derive approaches for their prevention. The main objective of this topical report is to study CCF events with intersystem dependencies. This report summarises the workshop results and presents CCF defence aspects for these events.

The objectives of this report are:

- to describe the data profile of the ICDE intersystem events;
- to develop qualitative insights into the events, expressed by event causes, coupling factors, corrective actions;
- to identify the type of dependencies between systems;
- to identify areas of improvement and possible or actual prevention mechanisms;
- to form lessons learnt and recommendations for CCFs with intersystem dependencies.

Section 2 presents the identification process of events. Section 3 describes the developed classification of the events. Section 4 presents an overview of the included events with their event parameters. Section 5 contains the engineering insights about the CCF events, supported by the failure mechanism descriptions. Section 6 provides a summary and conclusions. References are found in Section 7.

The ICDE project was organised to exchange CCF data among countries. A brief description of the project, its objectives, and the participating countries is given in Annex A. Annex B and Annex C present the definition of common-cause failures and the ICDE event definitions. Annex D presents the workshop form that was used in the event analysis.

2. Identification of events

The selection of intersystem events was based on keywords and event coding in the ICDE database to screen out candidates. The keywords were applied in the database fields C5 Description, C7 Event Interpretation, C13 Justification in the CCF view, and in the field Analyst Comments in the failure analysis view. Events previously marked with interesting event code eight, Multiple systems affected, are included. In addition, events were provided by the countries (ICDE members).

Keywords (occurrence)	
Multiple (5)	Multiple CCCG (1)
Some (4)	Different group (1)
Different system (4)	Branch connection (1)
Other system (4)	Also affected (1)
Many (2)	Different CCCG (1)
Multiple system (2)	Other CCCG (1)
In other (2)	Different CCF (1)
Different component (2)	Interconnection (1)

In total, the event set includes 25 intersystem event candidates (out of about 1 800 ICDE events). For some of these events, there exist correlated events in the database (eight events), see Table 2.1. ICDE events and intersystem events per component type

Table 2.1. ICDE events and intersystem events per component type

Component type	ICDE events	Intersystem events
Battery	1	1
Breakers	4	2
Centrifugal Pumps	12	9
Check valves	4	2
Diesels	5	4
Heat Exchanger	2	2
Level measurement	1	1
Motor Operated Valves	4	4
Total	**33**	**25**

3. Classification of events

Definition of a *CCF intersystem dependency event*

Events where a single CCF mechanism affects multiple systems. That is, events where a single CCF mechanism affected components in more than one different system or affected more than one different safety function.

Level of intersystem dependency and simultaneity factor

For classification of intersystem dependency events, two parameters were considered; the degree of failure and degree of simultaneity. The level of intersystem dependency impairment (severity) is determined by assessing how multiple systems were affected and degraded. The "simultaneity" (time factor) of the intersystem events is determined by the time frame between detection of the intersystem events. By combining these, the following classification was concluded and is used for the presentation of the workshop results.

- *Actual intersystem dependency*. Failures affecting multiple systems with a high time factor. Observed event(s) show evidence of multiple systems affected.
- *Partial/Incipient intersystem dependency*. Failures and/or impairment affecting multiple systems with a low time factor. Observed event(s) show evidence of multiple systems affected by similar problem (failure mechanism), e.g. same sub-component.
- *Potential intersystem dependency*. Failures in one system only, but other systems could have been affected due to the nature of the failure mechanism. Observed event(s) show evidence of potential intersystem dependency.

In addition, some of the included events showed that multiple common-cause component groups (CCCGs) were affected, yet all affected CCCGs belong to one system. For these events, the above-mentioned classification scheme is extended by:

- *Inter-CCCG dependency*. Failures of multiple CCCGs in only one system with no indications that other systems might have also been affected. These are not ordinary intersystem events but are interesting since they involve dependencies between CCCGs.

The result of the classification is presented in Section 5.2.

4. Overview of database content

This chapter presents an overview of the data set, which includes 25 intersystem CCF events. Tables exhibiting the event count for each of the event parameters (component type, event cause, coupling factor, corrective action, CCF root cause, detection method, and event severity) are presented. It should be noted that due to the low number of intersystem dependency events any statistical conclusion has to be interpreted carefully. At the time of writing the ICDE database includes 1 815 ICDE events, of which 162 are complete CCF events. The event parameters are defined in the ICDE general coding guidelines (NEA, 2019), see Annex C.

4.1 Component type and event severity

The scope of the workshop and the distribution of the event severity (NEA, 2019) is presented in Table 4.1. Figure 4.1 shows the distribution of component types.

Table 4.1. The scope of the workshop and distribution of component types per event severity

	Event severity								
Component type	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	**Total**	**Percent**	**Relative Occurrence**
Battery			1				1	4%	90%
Breakers			1	1			2	8%	130%
Centrifugal Pumps	2		1	3	1	2	9	36%	160%
Check valves		1				1	2	8%	120%
Control Rod Drive Assembly							0	0%	0%
Diesel generators	1		2			1	4	16%	120%
Fans							0	0%	0%
Heat Exchanger			1	1			2	8%	260%
Level measurement			1				1	4%	50%
Motor Operated Valves		1	2		1		4	16%	170%
Safety and Relief Valves							0	0%	0%
Total	**3**	2	**9**	**5**	**2**	**4**	**25**	**100%**	
Percent	**12%**	**8%**	**36%**	**20%**	**8%**	**16%**	**100%**		
Relative Occurrence	**130%**	**60%**	**130%**	**110%**	**30%**	**780%**			

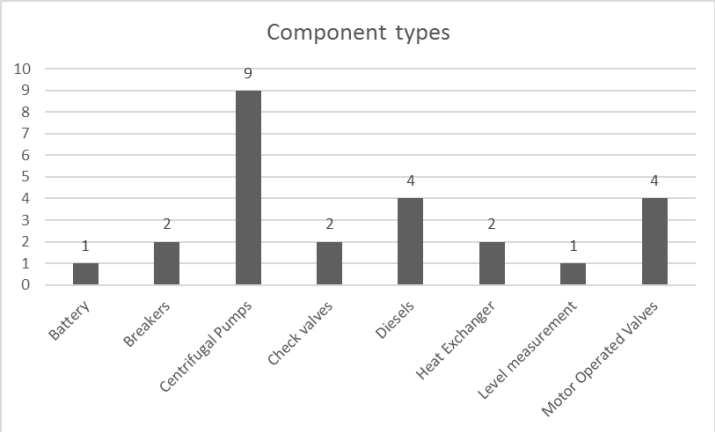
The most common component types are centrifugal pumps, motor operated valves, diesels and breakers. The most common event severities[1] are "CCF impaired" (36%)

1. For some events, there exist correlated events in the database (eight events). In these cases, the degree of severity is presented for one event.

and “complete impairment” (20%). The share of “complete CCFs” (12%) events is about the same compared to the total database, in which about 9% are complete CCFs.

To put the percentages in context, two values are given. “Percent” is the percentage in relation to the subset of events which was analysed in the workshop. “Relative occurrence” is the occurrence factor of the event parameter in relation to the complete ICDE database content. Taking the low overall number of events into account, there are, apart from a high share of “single impairment” events, statistically relevant deviations regarding event severity and component type between the complete dataset in the ICDE-database and the sub-set analysed for that report.

Figure 4.1. Distribution of component types



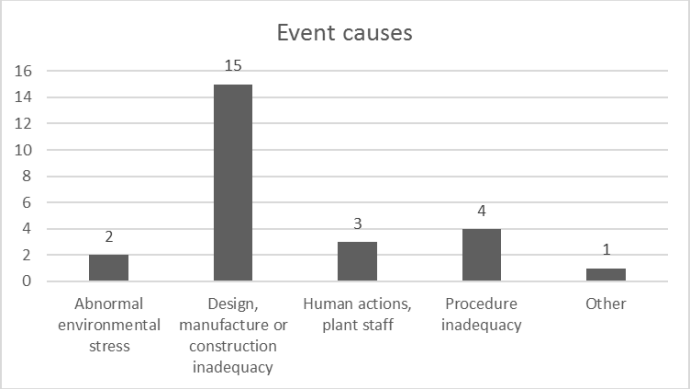
4.2 Event cause (apparent cause)

Table 4.2 and Figure 4.2 present the distribution of the apparent event causes. The event cause “design, manufacturer and construction inadequacies” was the most common in the event set.

Table 4.2. Distribution of event causes per severity category

	Event severity							
Event Cause	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	**Total**	**Percent**
Abnormal environmental stress	1		1				2	8%
State of other component(s)							0	0%
Design, manufacture or construction inadequacy		2	5	3	1	4	15	60%
Internal to component, piece part							0	0%
Human actions, plant staff	1		1	1			3	12%
Maintenance							0	0%
Procedure inadequacy	1		1	1	1		4	16%
Other			1				1	4%
Total	**3**	**2**	**9**	**5**	**2**	**4**	**25**	**100%**

Figure 4.2. Distribution of event causes



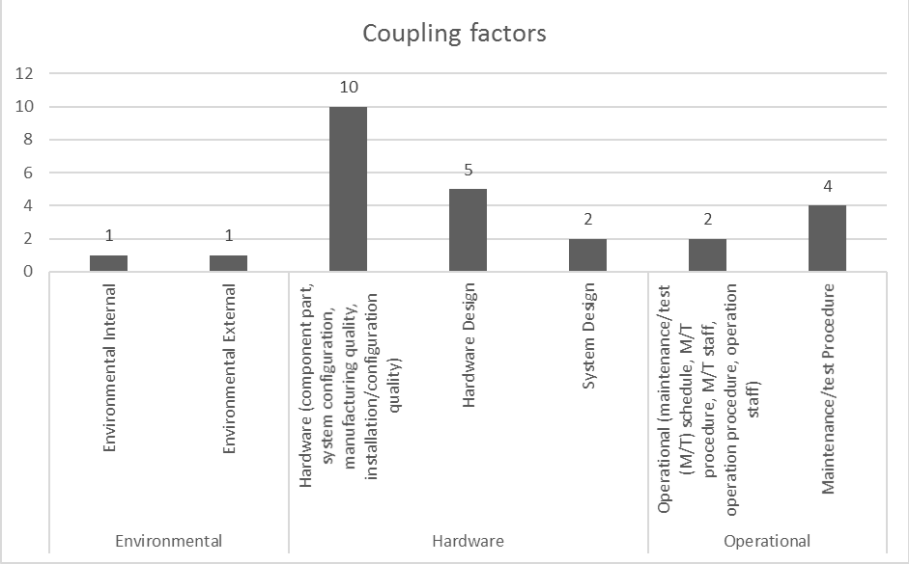
4.3 Coupling factor

Table 4.3 and Figure 4.3 show the distribution of the events by coupling factor. The coupling factor "hardware" was the most common factor in the event set.

Table 4.3. Distribution of coupling factors per severity category

	Event severity							
Coupling factor	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	**Total**	**Percent**
Environmental	**1**			**1**			**2**	8%
Environmental internal	1						1	4%
Environmental external				1			1	4%
Hardware		**2**	**7**	**2**	**2**	**4**	**17**	68%
Hardware (component part, system configuration, manufacturing quality, installation/configuration quality)		2	4	1	2	1	10	40%
Hardware design			1	1		3	5	20%
Hardware quality deficiency							0	0%
System design			2				2	8%
Operational	**2**		**2**	**2**			**6**	24%
Operational (maintenance/test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)	1			1			2	8%
Maintenance/test procedure	1		2	1			4	16%
Maintenance/test schedule							0	0%
Maintenance/test staff							0	0%
Operation procedure							0	0%
Operation staff							0	0%
Total	**3**	**2**	**9**	**5**	**2**	**4**	**25**	**100%**

Figure 4.3. Distribution of coupling factors



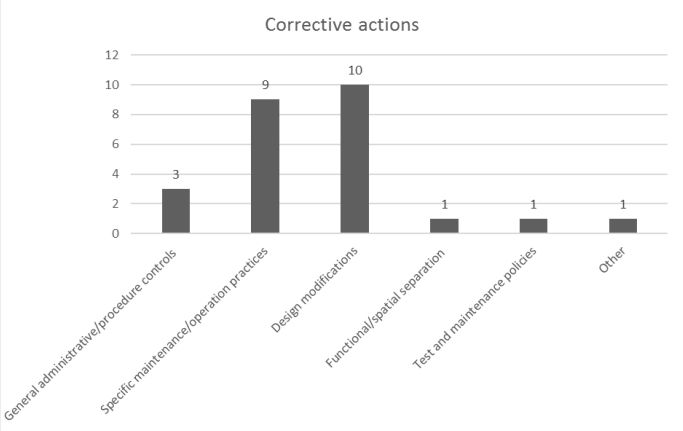
4.4 Corrective action

Table 4.4 and Figure 4.4 show the distribution of the events by corrective action. The most common corrective actions were “specific maintenance/operation practices” and “design modifications”.

Table 4.4. Distribution of corrective actions per severity category

	Event severity							
Corrective action	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	**Total**	**Percent**
General administrative/procedure controls	1	1	1				3	12%
Specific maintenance/operation practices	1		2	3	1	2	9	36%
Design modifications		1	4	2	1	2	10	40%
Diversity							0	0%
Fixing of component							0	0%
Functional/spatial separation	1						1	4%
Test and maintenance policies			1				1	4%
Other			1				1	4%
Total	**3**	**2**	**9**	**5**	**2**	**4**	**25**	**100%**

Figure 4.4. Distribution of corrective actions



4.5 CCF root cause

The root cause is *"the most fundamental reason for an event or adverse condition, which if corrected will effectively prevent or minimise the recurrence of the event or condition.*[2]*"* By combining the coded information for the (apparent) event cause, the corrective action and the coupling factor, insights regarding the *CCF root cause* of the events can be gained. The combination of the event parameters provides individual *root cause aspects*, which are combined into one CCF root cause. The possible CCF root cause aspects are:

- Deficiencies in the design of components or systems (Design).
- Deficiencies in procedures (Procedures).
- Deficiencies in human actions (Human actions).

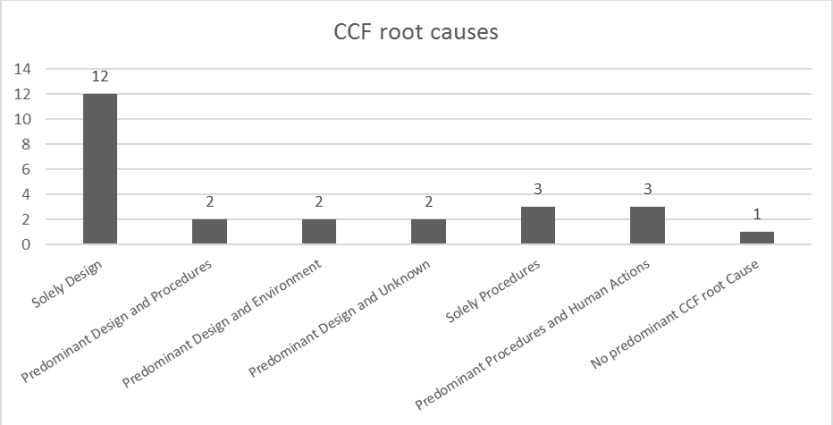
In addition to these three basic aspects, the "environmental" and "unknown" supporting aspects are used in case of events that are due to external factors or are not completely coded. It is noted if all three aspects of an event are identical (e.g. 3 x Design) or if there is a predominant and a contributing root cause aspect (e.g. 2 x design and 1 x procedure). Details on how the CCF root cause aspects are determined are given in the ICDE general coding guideline (NEA, 2019). The results of the CCF root cause assignment given in Table 4.5 and Figure 4.5 show the most common CCF root cause was "solely or predominantly design" (72%), i.e. root cause aspects with deficiencies in the design of components or systems. For the more severe events, i.e. complete CCF and complete impairment, procedure deficiency was the dominant CCF root cause.

2. See IAEA (2015) for more details.

Table 4.5. Distribution of CCF root causes per severity category

	Event severity							
CCF root cause	Complete CCF	Partial CCF	CCF Impaired	Complete Impairment	Incipient Impairment	Single Impairment	**Total**	**Percent**
Solely or predominantly design	**1**	**2**	**7**	**2**	**2**	**4**	**18**	**72%**
Solely Design		1	4	2	1	4	12	48%
Predominantly Design and Procedures		1			1		2	8%
Predominantly Design and Environment	1		1				2	8%
Predominantly Design and Unknown			2				2	8%
Solely or predominantly procedures	**2**		**2**	**2**			**6**	**24%**
Solely Procedures	1		1	1			3	12%
Predominantly Procedures and Human Actions	1		1	1			3	12%
No predominant CCF root Cause				**1**			**1**	**4%**
Total	**3**	**2**	**9**	**5**	**2**	**4**	**25**	**100%**

Figure 4.5. Distribution of CCF root causes



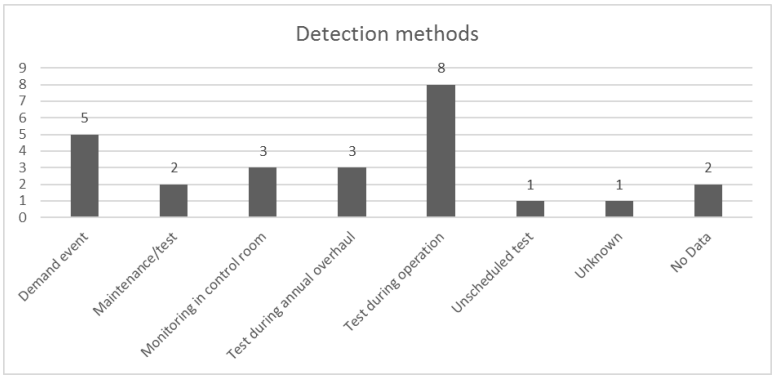
4.6 Detection method

Table 4.6 and Figure 4.6 show the distribution of the events by detection method. The most common detection method was “test during operation”, followed by “demand event”. All three complete CCFs were detected by a demand event.

Table 4.6. Distribution of detection methods per severity category

	Event severity							
Detection method	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	**Total**	**Percent**
Demand event	3		2				5	20%
Maintenance/test		1		1			2	8%
Monitoring in control room			2	1			3	12%
Monitoring on walkdown							0	0%
Test during annual overhaul			1	1		1	3	12%
Test during operation			4	1	1	2	8	32%
Unscheduled test				1			1	4%
Unknown						1	1	4%
No Data		1			1		2	8%
Total	**3**	**2**	**9**	**5**	**2**	**4**	**25**	**100%**

Figure 4.6. Distribution of detection methods



5. Engineering aspects of the collected events

The engineering aspects of the analysed events are presented in this chapter. The analysis was performed according to the workshop form in Annex D. A total of 25 events are included in the statistics in the following sections. The engineering aspects of the event analysis consist of:

- What has happened?
  - Classification of intersystem dependencies (see also Chapter 3).
  - Intersystem dependency factor.
  - Plant state when the event(s) was detected.
  - Failure mechanism descriptions.
  - Interesting event categories.
- What can be done to prevent this from happening again?
  - Actual and possible defences.
  - Areas of improvement.

5.1 Assessment basis

Failure mechanism description

The failure mechanism describes 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. It is derived from the event description and should preferably consist of one sentence.

Intersystem dependency classification and its dependency factors

The intersystem dependency events are classified according to Chapter 3.

The intersystem dependency factor describes the shared cause in the observed event(s). The factors are determined from the alternatives in Annex D.

Plant state when the event was detected

A part of the event analysis is to identify the plant state when the event was detected. This information can provide a sense of the severity of the events. Typical plant states are: at power, shutdown, and outage. Sometimes, the narrative event description may not specify the plant state.

Actual defence

The identification of actual defences aims to find what prevented all components from failing (if that was the case). Often, this aspect is difficult to identify, even when not all components are affected by the event. The detection of the event is often the only indicator of the prevention, and it is difficult to assess whether it was the design itself

or the observed failure mechanism preventing failure of all components in the group. In other cases, it may only be by accident or luck that not all components failed.

Areas of improvement

The areas of improvement section looks at what could prevent the event from happening again. It can be considered as lessons learnt from the event analysis and identifies possible defences to prevent the occurrence of CCFs. The available areas to choose from are: a) Design of system or site; b) Design of component; c) Surveillance of component and Maintenance procedure for component; d) Testing procedure; e) Operation procedure for component; and f) Management system of plant. An event can be applied to several areas.

Interesting event categories

The analysis also includes pointing out interesting and extraordinary CCF event records in the ICDE database, such as subtle dependencies with specific codes and descriptions. These records are important dependency events which are useful for the overall operating experience and can also be used as input for the stakeholders to develop defences against CCF. Several areas may be relevant for a single event.

5.2 Classification of intersystem dependencies

To explain why the event resulted in an intersystem CCF event, the observed dependencies and failure mechanism aspects need to be identified and analysed. The observed intersystem dependencies cover many types of aspects and these are categorised and presented in the following sub-sections. The main observed intersystem dependency aspects were:

- External events in which multiple systems (and units in some cases) were affected.
- Internal events in which multiple systems were affected due to identical or similar component design, same component protection settings, or identical maintenance (such as the same type of grease).

The level of intersystem dependency was determined by identifying the degree of system impairment, simultaneity (time factor) and intersystem dependency factors (internal or external, see further in Table D.1), which is presented in Table 5.1. The definitions for the different types of intersystem dependency are given in Section 3.

Table 5.1. Level of intersystem dependency

Level of Intersystem dependency	Internal factor	External factor	Total
A: Actual intersystem dependency	8	3	11
B: Partial/Incipient intersystem impairment	4		4
C: Potential intersystem impairment	2	2	4
D: Multiple CCCGs in one system	6		6
Total	**20**	**5**	**25**

The 11 actual intersystem dependency events make up about 0.6% of the whole ICDE database, which consists of about 1 800 events. About 9% of the severe events in the

total ICDE database are complete CCFs and the three complete CCF intersystem events include about 1.8% of the complete CCFs, see further Section 0.

The following sub-sections present all events for each level with their failure mechanism description and possible improvement to prevent the event from happening again.

5.2.1 Actual intersystem dependency

This section presents the identified intersystem dependency aspects for events classified as an actual intersystem dependency, in which multiple systems were affected.

Three intersystem events failure mechanisms were related to external events:

Failure mechanism description	***Improvement***
– Clogging due to foliage-polluted high river water affected heat exchangers in both the nuclear and the conventional service water system.	➢ Design of system or site.
– Two complete CCFs, see section 5.5.	

Three intersystem events failure mechanisms were related to component protection settings:

Failure mechanism description	***Improvement***
– Breakers in different groups fail to close due to misadjustment of overcurrent protection set points.	➢ Introduce a process to ensure the quality of maintenance procedure or testing procedure with actual voltage conditions.
– The set points of overcurrent protection devices of pump motors in the residual heat removal and the nuclear and primary reactor containment building ventilation systems were set too low to cover all demand cases.	➢ Maintenance procedure – check of set points.

Five intersystem events failure mechanisms were related to wear and degradation of components:

Failure mechanism description	***Improvement***
– The same type of breaker (but not identical) with a mechanical problem (the breaker bounced several times which caused the pump to trip), which was used in multiple systems. The event was a recurrent single event.	➢ Introduce diverse breaker types or better design of breakers.
– Incompatible mixtures of grease were found at different pump bearings in the Medium Pressure Safety Injection System and the Containment Spray System.	➢ Quality of maintenance procedure or staggered maintenance. Diversification of maintenance staff is also a possible defence.

Failure mechanism description	*Improvement*
– Cable connectors of 0.4 kV pump motors in two different systems were not capable of frequent component operation (thermal stress due to the frequent inrush-currents which are much higher than the currents during continuous load).	➢ Improve the design of the connector to allow for frequent operations.
– Frequent pulling of plug connectors in the power supply degraded the contact pins and caused an interruption of the power supply of the valve's actuator. The same type of impairment was detected in other systems (outside the ICDE database).	➢ Consider degradation due to the testing procedure for the expected life-time of the piece part.
– Compensators which were used in the inlet air system of two different emergency diesel generator (EDG) groups were improperly installed which caused parts of them to come loose and damage the turbochargers.	➢ The event would have been prevented by paying attention to parts that could eventually get loose. The intersystem dependency could have been avoided by using diverse diesel designs.

As for the identified intersystem dependency factors, the external events were correlated by proximity, i.e. common intake channel. Most of the internal events were correlated by design, i.e. same type of component but not always identical. Some events were also correlated by shared components, the type of operation of components and identical maintenance procedures.

5.2.2 Partial/Incipient intersystem dependency

The identified intersystem dependency aspects for events classified as a partial/incipient intersystem dependency, in which multiple systems were affected, were:

Failure mechanism description	*Improvement*
– Corrosion of plates in two battery systems (same failure mechanism) with the same design. The cause of the corrosion was an excessive chloride-acid concentration of the electrolyte. The chloride was dissolved from the support elements inside the batteries.	➢ Improve testing procedure and the scope of maintenance of these components.
– Damage of a certain resistor on multiple I&C-cards due to thermal overload caused a delayed start of two pumps in different systems with the same design.	➢ Unclear.
– Improper material of motor pinion keys caused degradations in the drive units of motor operated valves (MOVs) of the same design used in multiple systems.	➢ Unclear.
– Weak dimensioning of locking pins at several MOVs with same design used in multiple systems.	➢ Better component design.

All four partial/incipient intersystem events were attributed to inadequate component design with problems with different piece parts and inadequate material.

5.2.3 Potential intersystem dependency

The identified intersystem dependency aspects for events classified as a potential intersystem dependency, in which multiple systems could have been affected, were:

Failure mechanism description	*Improvement*
– Ageing of damping elements in several breakers with identical design, which were used in multiple systems.	➢ Improve test intervals.
– Mussels and mud were detected in a branch connection between the Essential Service Water System (ESWS) and the Auxiliary Feed Water System (AFWS). This connection is used only in emergency situations when the steam generators have to be fed with raw water via the ESWS. Only the AFWS pumps were degraded and the ESWS was not affected.	➢ To define a periodic cleaning procedure for ESWS branch connections.
– An external event where eels were clogging a cooling system. Other systems could have been affected as well.	➢ Improved planning of work activities.
– One complete CCF, see section 5.5.	

Among the potential intersystem events, one event shared system parts. In the other two events, identical design was the main correlation factor as well as some organisational factors, i.e. ageing and incorrect procedure.

5.2.4 Inter-CCCG events

The identified intersystem dependency aspects for events classified as inter-CCCG dependency (i.e. events in which multiple CCF groups in the same system are affected) were:

Failure mechanism description	*Improvement*
– Operational errors during switchover between different pumps in the feedwater system (modelled in different CCCGs) caused the failure of several pumps.	➢ Testing procedure.
– Mechanical wearing caused MOVs with an identical design used in the residual heat removal system to re-bounce after closure.	➢ Better components or improved (more frequent) maintenance or replacement of piece parts.
– Leakage of cooling water due to internal corrosion at the diesel turbocharger was observed for two diesel CCCGs.	➢ Better ageing management.
– Component parts of several MOVs in multiple CCCGs in the essential service water were missing.	➢ A better understanding of component parts would probably have prevented failure.

Failure mechanism description	*Improvement*
– Misadjusted settings of the fuel amount governor led to fluctuations in the rotation speed in the start-up process and thereby to the shut-off of the diesel at two diesel CCCGs. Both diesel CCCGs use an identical design of the fuel amount governors.	➢ Design of component.
– Poor contact between the cable grip and the cable in the feeding device for the joint ground voltage resulting in an interruption of the level indication in two CCCGs. A contributing factor was the identical installation.	➢ Design of system – remove cross-connection of components to the same zero voltage feed.

For the inter-CCCG events, the main issue involved defective material (i.e. mechanical wear, leakage due to corrosion and poor contacts). The other issues were wrong settings, missing component parts, and one external event due to clogging.

5.3 Plant state when the event(s) was detected

Table 5.2 presents the plant state when the event(s) was detected. The information about the plant state is not considered essential in this engineering review. However, it gives the reader a sense of when the events occurred and whether any trend is seen for the intersystem events. The most common plant state was "at power", followed by "outage". Four out of ten actual intersystem events occurred at power. Inter-CCCG events were observed at power and during outage.

Table 5.2. Plant state when the events were detected

Plant state	Count	Percent
At power	11	44%
Shutdown	1	4%
Outage	7	28%
Other	2	8%
Unknown	4	16%
Total	**25**	**100%**

5.4 Interesting event categories

Table 5.3 presents the statistics per interesting event code, which are defined in the ICDE general coding guidelines (NEA, 2019), see Annex C.

Table 5.3. Applied interesting event codes

Interesting CCF event codes	No. of events
Complete CCF	3
CCF Outside planned test	0
Component not-capable	1
Multiple defences failed	0

Interesting CCF event codes	No. of events
Sequence of multiple CCF mechanisms	0
Multiple systems affected	15
Common-Cause Initiator	2
Safety culture	1
Multi-Unit CCF	6
No code applicable	5
Questionable coding	1
Total codes	**34**

The applied interesting event codes provided some insights:

Multiple systems affected: The high number of events in this category reflects this workshop topic and are presented in Section 5.2. The potential intersystem events and the inter-CCCG events were not assigned to this event code.

Complete CCF: The complete CCF events are presented in Section 0. None of the events had "solely design" as CCF root cause.

Multi-unit CCF: Six events were determined to be multi-unit CCFs, in which four events were classified as actual intersystem dependency events.

Safety culture: One event was assessed as related to safety culture. The event was a pump event where operational errors during switchover between different pumps in the feedwater system (modelled in different CCCGs) caused the failure of several pumps. The event was assessed as an inter-CCCG event (see Section 5.2.4) and the "intersystem" dependency was several operational factors, i.e. incorrect procedure, misinterpretation of requirements, incorrect technical specification, misunderstanding of system configuration/function. Thus, the event was assessed to be an interesting safety culture event.

Component not capable: One event was assessed as not capable to perform its function over a long period of time. The event involved MOVs where the failure mechanism was the wrong setting of torque limit switches and the not-capable part was the torque limiting device. The event was assessed as an actual intersystem event (see Section 5.2.1) and the intersystem dependency factors were incorrect procedure and same design.

Common-cause initiator (CCI): Two events were assessed as CCIs.

- The first event was a potential intersystem external event (see Section 5.2.3) where heat exchangers were clogging in a cooling system due to eels. Due to the nature of the failure mechanism, other systems could have been affected as well. The interesting CCI aspect was that the event happened during the outage period so this event would only be relevant as a CCI in a shutdown PRA model.
- The second event was assessed not only as an actual intersystem dependency event (see Section 5.2.1) but also as a CCI. A very high water level of the river combined with a high amount of foliage and grass led to clogging of the tube sides of the nuclear and conventional service water heat exchangers. As to prevent reoccurrence, a change in system design was suggested.

5.5 Lessons learnt from complete intersystem CCFs

The engineering analysis identifies actual CCF defences that were present in the events and possible improvements to defences. The defences aim to prevent all components from failing or the event from happening again. In this section, possible defences are identified for the complete CCFs. In these events, all impacted components failed completely, so no effective CCF defences were present. A possible defence is used to identify what to improve to reduce the risk of the event happening again. The actual defences observed in non-complete CCFs are discussed in Section 5.6. Each possible defence is assigned to one of the categories given in the workshop form, as shown in Annex D. A total of three events were complete intersystem CCFs.

- The first intersystem event was a pump event where the charging pump service water pumps become air-bound due to maintenance activities due to an incorrect procedure, which also affected the main control room (MCR) chiller pumps belonging to a non-safety related system. An introduction of a process to ensure the quality of the maintenance procedure was suggested as an improvement.
- The second intersystem event was a diesel event where a large school of fish impinging on the intake screens of the essential service water systems caused screens to fail and caused the clogging of the EDG heat exchangers. The event affected the circulating water system (CWS) and the ESWS at two units simultaneously. To prevent reoccurrence, improved surveillance of intake screens and improved operational response to clean intake screens was suggested.
- The third intersystem event was a pump event where erroneous modifications to the AFWS start logic caused multiple pumps in the component cooling water system (CCWS) 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 against this type of event. An improved process for work preparations and better quality assurance (QA) of documentation would also have helped.

5.6 Lessons learnt from actually observed defences

For the non-complete CCF events, the task was to identify actual defences. An actual defence is a defence that prevented the event from becoming more severe, i.e. it identifies what prevented all components from failing. Each actual defence should be assigned to one of the categories given in the workshop form in Annex D.

Examples of actual defences, i.e. what prevented the event from developing into a complete CCF:

- Incompatible mixtures of grease were found at different pump bearings in the medium pressure safety injection system and the containment spray system (see Section 5.2.1). The observed actual defence was the detection of unusual noise during a routine test.
- Compensators which were used in the inlet air system of two different EDG groups were improperly installed which caused parts of them to come loose and

damage the turbochargers (see Section 5.2.1). The actual defence was the routine testing programme for the EDGs in combination with slow progression of the failure mechanism.

- Several MOVs with the same design were used in multiple systems and were found with weak dimensioning of locking pins (see Section 5.2.2). The actual defence were adequate subsequent inspections after the first finding.

5.7 Areas of improvement

For the non-complete CCF events, the task was also to identify areas of improvement to reduce the risk of the event happening again. There were six areas of improvement to choose from, and an event could be assigned to multiple areas, which affects the event count. Table 5.4 presents the distribution of intersystem dependencies per area of improvement for non-complete CCFs. The most common areas of improvement were "testing procedure", "surveillance of component and maintenance procedure for component" and "management system of plant". The event-specific improvements are presented in Section 5.2.

Table 5.4. Distribution of intersystem dependency per area of improvement for non-complete CCFs

	Areas of improvement					
Level of Intersystem dependency	a – Design of system or site	b – Design of component	c – Surveillance of component and Maintenance procedure for component	d – Testing procedure	e – Operation procedure for component	f – Management system of plant[3]
A: Actual intersystem dependency	1	3	4	1		4
B: Partial/Incipient intersystem impairment		1		1		
C: Potential intersystem impairment			1	1		1
D: Multiple CCCGs in one system	2	2	1	1		2
Total marks	**3**	**6**	**6**	**4**		**7**

5.8 Workshop with the Nordic PSA Group

In addition to the ICDE workshop, a workshop was organised in October 2018 with the Nordic PSA Group (NPSAG), where PSA specialists analysed the events classified as actual intersystem dependencies from a PRA modelling and quantification perspective.

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

The workshop focused on the following questions:

- What information about intersystem CCF is available in ICDE data? How can it be used to define CCF groups?
- From the observed failure mechanism can you establish rules for how or when to define or not to define intersystem CCF groups?

The noteworthy conclusions from the discussions were:

- The events are only identified through the descriptive fields in the ICDE database. Thus, no marking of intersystem dependencies is included in the data collection to specify the intersystem dependency. The importance of having intersystem requirements when reporting events should be addressed.
- The experience feedback to the PRA practitioners and others is important since intersystem events are rare.
- The intersystem dependency modelling will have different importance depending on the application, e.g. single-unit PSA, shutdown PRA or multi-unit PRA, and being a CCI in some applications. Thus, a different set of groups will be dependent or applicable based on the application/model.
- Some events show evidence that they could be explicitly modelled. However, other failure mechanisms show evidence of the need to have intersystem CCF groups, see Table 5.5 Several event causes were observed, and the failure mechanism has a very central role to determine and define how and if an intersystem CCF group is needed. Also, the failure mechanism categorisation can be used to evaluate the modelling approach to avoid double counting or to ensure completeness.
- An intersystem CCF cut-off value could be used to both estimate and to represent the dependency between two CCF group, i.e. one way to quantify the maximum credit for diversity.

Table 5.5. Possible modelling approach in component fault tree model for intersystem CCF events

CCF root cause / Modelling approach	Deficiencies in the design of components or systems (D)	Procedural or organisational deficiencies (P)	Deficiencies in human actions (H)
Explicit modelling			
Intersystem dependencies	In functional fault trees or Event Trees (ET)	Pre-initiator Human Reliability Analysis (HRA) and Human Failure Event (HFE) in ET	
CCCG modelling			
Intersystem CCF	Dependent on the failure mechanism? For example, the failure mechanism categories defined in the ICDE general coding guidelines (NEA, 2019).		

6. Summary and conclusions

The workshop included 25 intersystem dependency events. The main objective of this topical report was to study CCF events with intersystem dependencies, i.e. events with a single common-cause failure mechanism that affects components in more than one different system.

The following classification was concluded and used for the presentation of the workshop results.

- *Actual intersystem dependency:* failures affecting multiple systems with a high time factor.
- *Partial or incipient intersystem dependency:* failures and/or impairments affecting multiple systems with a low time factor.
- *Potential intersystem dependency:* failures in one system only, but other system(s) could have been affected due to the nature of the failure mechanism.
- *Inter-CCCG dependency events:* failures of multiple CCCGs in only one system with no indications that other systems are affected.

The first and most important insight of the analysis is that intersystem CCFs actually exist and that they are well documented in the operating experience.

Summary of database content:

- The most common component types were Centrifugal Pumps, Motor Operated Valves, Diesels and Breakers.
- The most common event severities were “CCF impaired” (36%) and “complete impairment” (20%).
- The event cause “design, manufacturer and construction inadequacies” was the most common cause.
- The coupling factor “hardware” was the most common factor.
- The most common corrective actions were “specific maintenance/operation practices” and “design modifications”.
- The most common CCF root cause was “solely or predominantly design” (72%), i.e. root cause aspects with deficiencies in the design of components or systems.
- For the more severe events, i.e. complete CCF and complete impairment, was procedure deficiency the dominating CCF root cause.
- The most common detection method was “test during operation” followed by “demand event”. All three complete CCFs were detected by demand event.

Summary of the engineering aspects:

The event set shows evidence of observed:

- External intersystem events in which multiple systems (and units in some cases) were affected.
- Internal intersystem events in which multiple systems were affected due to identical or similar component design, same component protection settings, or identical maintenance (such as the same type of grease).
- Inter-CCCG dependency events (i.e. events in which multiple CCF groups in the same system are affected).

In addition:

- Most of the events were correlated by identical design, i.e. the type of component was the same but not always identical. Some events were also correlated by shared components, the same type of operation of component and having the same maintenance procedure.
- Six events were determined to be multi-unit CCFs, in which four events were classified as actual intersystem dependency events.
- Three events were complete CCFs demand events and were classified as actual intersystem dependency events.
- Actual observed defences identified in the analysis were sufficient testing, surveillance of components during outage period, inspections after the first finding, observation of noise at routine test, sufficient recurrent testing, random examination, and slow failure process (e.g. corrosion).
- Different areas of improvement were identified for the events. In some cases, ensuring the quality of maintenance or testing procedures could have prevented the event. For others, specific design changes were proposed which corresponds with the corrective actions taken for the events.

The lessons learnt from the engineering aspects:

- Intersystem CCFs are rare events (the 25 events correspond to about 1.4% of all CCF events in the ICDE database, and about 1.9% of the complete CCFs or 0.02 in an intersystem β-factor model), yet their existence and their risk significance should not be overlooked.
- The observed intersystem dependency events cover a wide range of component types, systems and failure mechanisms. Thus, there are no component types which are especially vulnerable or robust against intersystem CCFs, i.e. no particular trend can be observed in the data.
- Highly redundant component types, such as SRV and CRDA, were not observed among the events (these components are not intersystem systems by design).
- Modification of component protection devices (overcurrent, torque, etc.) should be performed with great care. If possible, only one system redundancy should be modified until sufficient operating experience is gathered to ensure its adequacy.

- Maintenance or modification activities in one system resulting in a CCF in another system were observed. Sharp attention should be paid when planning maintenance or modification activities to ensure that the activities do not affect other systems.
- Diversity on the component level does not ensure diversity on piece part level in different systems. For example, the same type of breaker is used in multiple systems and is vulnerable to a CCF mechanism.
- Thus, intersystem dependencies could exist on a lower component level which is normally not considered in a PRA. Due to the risk significance intersystem dependencies should be taken into account when performing a PRA, while also considering the rarity of these events and credit for defences that could prevent or mitigate their occurrence.

7. References

IAEA (2015), "Root Cause Analysis Following an Event at a Nuclear Installation: Reference Manual", IAEA-TECDOC-1756, International Atomic Energy Agency, Vienna, www.iaea.org/publications/10626/root-cause-analysis-following-an-event-at-a-nuclear-installation-reference-manual.

NEA (2019), "Technical Note on the ICDE Project General Coding Guidelines", ICDE, Issue 3, January 2019 (not publicly available).

Glossary

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

CCF intersystem dependency event: Events where a single CCF mechanism affects multiple systems. That is, events where a single CCF mechanism affected components in more than one different system or affected more than one different safety function.

CCF root cause: The CCF root cause is the most fundamental reason for the observed common-cause failure. It is derived by combining coded information from the event description in the ICDE database (event cause, corrective action and the coupling factor). Depending on the coding, the possible CCF root cause aspects are "deficiencies in the design of components or systems", "procedural or organisational deficiencies", or "deficiencies in human actions".

Coupling factor: The coupling factor field describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected.

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 event cause and/or coupling factor between the impairments.

Defence: Any operational, maintenance, and design measures taken to diminish the probability and/or consequences of common-cause failures.

Detection method: The detection method describes how the exposed components were detected.

Event cause: In the ICDE database, the event cause describes the direct reason for the component's failure. For this project, the appropriate code is the one representing the common cause, or if all levels of causes are common cause, the most readily identifiable cause.

Event severity: The severity category expresses the degree of severity of the event based on the individual component impairments in the exposed population.

Failure mechanism: Describes the observed event and influences leading to a given failure. Elements of the failure mechanism could be a deviation or degradation or a chain of consequences. It is derived from the event description.

ICDE event: Refers to all events accepted into the ICDE database. This includes events meeting the typical definition of CCF event (as described in Annex B). ICDE events also include less severe events, such as those with impairment of two or more components (with respect to performing a specific function) that exists over a relevant time interval and is the direct result of a shared cause.

Interesting CCF event categories: Marking of events as interesting via event codes. The idea of these codes is to highlight a small subset of ICDE events which are in some way "extraordinary" or provide "major" insights.

Inter-CCCG dependency: Failures of multiple CCCGs in only one system with no indications that other systems might have also been affected. These are not ordinary intersystem events but are interesting since these involve dependencies between CCCGs.

Annex A – Overview of the ICDE Project

Annex A contains information regarding the ICDE project.

Background

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 several 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 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 ICDE project was initiated in August 1994. The NEA has formally operated the project over seven consecutive terms from 1998 to 2018. The current term started in 2019 and is due to run until the end of 2022. Member countries under the current agreement between the NEA and the organisations representing them in the project are: Canada (CNSC), Czech Republic (UJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), the Netherlands (ANVS), Sweden (SSM), Switzerland (ENSI), and the United States (NRC). Other member countries have participated in previous phases of the project. The previous member countries include: Korea (KAERI), Spain (CSN), and the United Kingdom (ONR). The CCF data contributed by previous member countries continues to be used to inform the analyses performed by the ICDE project.

Information about the ICDE project can be found at the NEA website: www.nea.fr/html/jointproj/icde.html. Additional information can also be found at the web site https://projectportal.afconsult.com/ProjectPortal/icde.

Scope of the ICDE Project

The ICDE project aims to include all possible events of interest, comprising complete, partial, and incipient CCF events, called "ICDE events" in this report. The project covers the key components of the main safety systems, including centrifugal pumps, diesel generators, motor operated valves, power operated relief valves, safety relief valves, check valves, main steam isolation valves, heat exchangers, fans, batteries, control rod drive assemblies, circuit breakers, level measurement and digital instrumentation and control (I&C) equipment.

Data Collection Status

Data are collected in an MS.NET-based database implemented and maintained at ÅF, Sweden, the appointed ICDE Operating Agent. The database is regularly updated. It is operated by the Operating Agent following the decisions of the ICDE Steering Group.

ICDE Coding Format and Coding Guidelines

Data collection guidelines have been developed during the project and are continually revised. They describe the methods and documentation needed to develop the ICDE databases and reports. The format for data collection is described in the general coding guidelines and in the component-specific guidelines. Component-specific guidelines are developed for all analysed component types as the ICDE plans evolve (NEA, 2019).

Protection of Proprietary Rights

Procedures for protecting confidential information have been developed and are documented in the Terms and Conditions of the ICDE project. The co-ordinators in the participating countries are responsible for maintaining proprietary rights. The data collected in the database are password protected and are only available to ICDE participants who have provided data.

Annex B – Definition of common-cause events

In the modelling of common-cause failures in systems consisting of several redundant components, two kinds of events are distinguished:

- Unavailability of a specific set of components of the system, due to a common dependency, for example on a support function. If such dependencies are known, they can be explicitly modelled in a PSA.
- Unavailability of a specific set of components of the system due to shared causes that are not explicitly represented in the system logic model. Such events are also called "residual" CCFs. They are incorporated in PSA analyses by parametric models.

There is no rigid borderline between the two types of CCF events. There are examples in the PSA literature of CCF events that are explicitly modelled in one PSA and are treated as residual CCF events in other PSAs (for example, CCF of auxiliary feedwater pumps due to steam binding, resulting from leaking check valves).

Several definitions of CCF events can be found in the literature, for example, in NUREG/CR-6268, Revision 1 "Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding"[4]:

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

A CCF event consists of component failures that meet four criteria: (1) two or more individual components fail, are degraded (including failures during demand or in-service testing), or have deficiencies that would result in component failures if a demand signal had been received; (2) components fail within a selected period of time such that success of the PRA mission would be uncertain; (3) components fail because of a single shared cause and coupling mechanism; and (4) components fail within the established component boundary.

In the context of the data collection part of the ICDE project, the focus will be on CCF events with total as well as partial component failures that exist over a relevant time interval[5]. To aid in this effort the following attributes are chosen for the component fault states, also called impairments or degradations:

- Complete failure of the component to perform its function.

4. Mosleh, A., T.E. Wierman and D.M. Rasmuson (2007), "Common-Cause Failure Database Collection and Analysis System: Event Data Collection, Classification, and Coding", NUREG/CR 6268, Revision 1, US Nuclear Regulatory Commission, Washington.

5. Relevant time interval: two pertinent inspection periods (for the particular impairment) or, if unknown, a scheduled outage period.

- Degraded ability of the component to perform its function.
- Incipient failure of the component.
- Default: component is working according to specification.

Complete CCF events are of particular interest. A "complete CCF event" is defined as a dependent failure of all components of an exposed population where the fault state of each of its components is "complete failure to perform its function" and where these fault states exist simultaneously and are the direct result of a shared cause. Thus, the ICDE project is interested in collecting complete CCF events as well as partial CCF events. The ICDE data analysts may add interesting events that fall outside the CCF event definition but are examples of recurrent – eventually non-random – failures. With a growing understanding of CCF events, the relative share of events that can only be modelled as "residual" CCF events is expected to decrease.

Annex C – ICDE General Coding Guidelines

Event cause

In the ICDE database, the event cause describes the direct reason for the component's failure. For this project, the appropriate code is the one representing the common cause, or if all levels of causes are common cause, the most readily identifiable cause. The following coding was suggested:

C State of other components. The cause of the state of the component under consideration is due to state of another component.

D Design, manufacture or construction inadequacy. This category encompasses actions and decisions taken during design, manufacture, or installation of components, both before and after the plant is operational. Included in the design process are the equipment and system specification, material specification, and initial construction that would not be considered a maintenance function. This category also includes design modifications.

A Abnormal environmental stress. This represents causes related to a harsh environment that is not within component design specifications. Specific mechanisms include chemical reactions, electromagnetic interference, fire/smoke, impact loads, moisture, radiation, abnormally high or low temperature, vibration load, and severe natural events.

H Human actions. This represents causes related to errors of omission or commission on the part of plant staff or contractor staff. This category includes accidental actions, and failure to follow procedures for construction, modification, operation, maintenance, calibration, and testing. This category also includes inadequate training.

M Maintenance. All maintenance not captured by H – human actions or P – procedure inadequacy.

I Internal to component or piece part. This deals with malfunctioning of internal parts to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the environment on the component. Specific mechanisms include corrosion/erosion, internal contamination, fatigue, and wear out or end of life.

P Procedure inadequacy. Refers to ambiguity, incompleteness, or error in procedures, for operation and maintenance of equipment. This includes inadequacy in construction, modification, administrative, operational, maintenance, test and calibration procedures. This can also include the administrative control procedures, such as change control.

O Other. The cause of the event is known, but does not fit one of the other categories.

U Unknown. This category is used when the cause of the component state cannot be identified.

Coupling factor

The ICDE general coding guidelines (NEA, 2019) define coupling factor as follows: "The coupling factor field describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected." For some events, the cause and the coupling factor are broadly similar, with the combination of coding serving to give more detail as to the causal mechanisms. The codes are selected from the following:

H Hardware (component, system configuration, manufacturing quality, installation, configuration quality). Coded if none of or more than one of HC, HS or HQ applies, or if there is not enough information to identify the specific "hardware" coupling factor.

HC Hardware design. Components share the same design and internal parts.

HS System design. The CCF event is the result of design features within the system in which the components are located.

HQ Hardware quality deficiency. Components share hardware quality deficiencies from the manufacturing process. Components share installation or construction features, from initial installation, construction, or subsequent modifications

O Operational (maintenance/test [M/T] schedule, M/T procedures, M/T staff, operation procedure, operation staff). Coded if none or more than one of OMS, OMP, OMF, OP or OF applies, or if there is not enough information to identify the specific "maintenance or operation" coupling factor.

OMS M/T schedule. Components share maintenance and test schedules. For example, the component failed because maintenance procedure was delayed until failure.

OMP M/T procedure. Components are affected by the same inadequate maintenance or test procedure. For example, the component failed because the maintenance procedure was incorrect or the calibration set point was incorrectly specified.

OMF M/T staff. Components are affected by maintenance staff error.

OP Operation procedure. Components are affected by inadequate operations procedure.

OF Operation staff. Components are affected by the same operations staff personnel error.

E Environmental, internal and external.

EI Environmental internal. Components share the same internal environment. For example, the process fluid flowing through the component was too hot.

EE Environmental external. Components share the same external environment. For example, the room that contains the components was too hot.

U Unknown. Sufficient information was not available in the event report to determine a definitive coupling factor.

Detection method

The ICDE general coding guidelines (NEA, 2019) suggest the following coding for the detection method for each failed component of the exposed population:

MW Monitoring on walkdown

MC Monitoring in control room

MA Maintenance/test

DE Demand event (failure when the response of the component(s) is required)

TI Test during operation

TA Test during annual overhaul

TL Test during laboratory

TU Unscheduled test

U Unknown

Corrective action

In the ICDE general coding guidelines (NEA, 2019) the "corrective actions field 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 event cause and/or coupling factor between impairments. Selection is made from the following codes:

A General administrative/procedure controls

B Specific maintenance/operation practices

C Design modifications

D Diversity. This includes diversity in equipment, types of equipment, procedures, equipment functions, manufacturers, suppliers, personnel, etc.

E Functional/spatial separation. Modification of the equipment barrier (functional and/or physical interconnections). Physical restriction, barrier, or separation.

F Test and maintenance policies. Maintenance programme modification. The modification includes item such as staggered testing and maintenance/ operation staff diversity.

G Fixing component

O Other. The corrective action is not included in the classification scheme.

CCF root cause

For each event, the cause, the corrective action and the coupling factor are assigned to one of the three basic CCF root cause aspects listed below:

- *Deficiencies in the design of components or systems (D):* This category comprises all events where safety-relevant components or systems were not available or otherwise impaired due to deficiencies in design. This although they were operated and maintained procedurally correctly and under circumstances (ambient temperature, fluid temperature, pressure etc.) within

the expected limits. In general, these events require changes to hardware as corrective action.

- *Procedural or organisational deficiencies (P):* This category comprises all events where a) wrong or incomplete procedures were applied and followed and b) events, which happened because of organisational deficiencies of one or more of the involved entities (utilities, subcontractors, TSO, regulating bodies etc.). In general, these events require changes to procedures or organisational improvements as corrective action.
- *Deficiencies in human actions (H):* This category comprises all events that happened because of human mistakes. Corrective actions for these events may involve training measures, further improvements of procedures and instructions or organisational improvements (e.g. more personnel).

The CCF root causes are further discussed in the ICDE general coding guidelines (NEA, 2019).

Event severity

The severity category expresses the degree of severity of the event based on the individual component impairments in the 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.

Interesting CCF event categories

Interesting CCF event codes	**Description** **Purpose**
Complete CCF **(1)**	Event has led to a complete CCF. This code sums up all complete CCFs, for any component type.

Interesting CCF event codes	Description Purpose
CCF Outside planned test **(2)**	The CCF event was detected outside of normal periodic and planned testing and inspections. The code gives information about test efficiency when CCFs are observed by other means than ordinary periodic testing – information about weaknesses in the defence-in-depth level 2.
Component not-capable **(3)**	The event revealed that a set of components was not capable of performing its safety function over a long period of time. The code gives information about a deviation from deterministic approaches when it is revealed that two or more exposed components did not perform the licensed safety function during the mission time.
Multiple defences failed **(4)**	Several lines of defence failed More than one line of defence against CCF failed e.g. in the QA processes of designer, manufacturer, TSO and utility during construction and installation of a set of components.
NO LONGER USED **CCF New Failure mechanism (5)**	The event revealed an unattended or unforeseen failure mechanism. The code gives information about a new CCF event revealed and a new failure mechanism, not earlier documented in the licensing documentation or operating history.
Sequence of multiple CCF mechanisms (6)	Events with a sequence of multiple CCF mechanisms. The code gives information about incidents which revealed that during the event sequence more than one CCF mechanism was observed. The code focuses on the sequence of failures in the observed CCF mechanisms, regardless of how many CCCGs were affected.
NO LONGER USED **CCF Causes Modification (7)**	Event causes major modification The code gives information about a CCF event revealed that has led to or will lead to a major plant or system or component modification.
Multiple Systems affected (8)	Events where a single CCF mechanism affected multiple systems. This code indicates events where a single CCF mechanism affected components in more than one different system or affected more than one different safety function. In most cases, these events are Cross Component Group CCFs (X-CCF).

Interesting CCF event codes	**Description** **Purpose**
Common-Cause Initiator (9)	A dependency event originating from an initiating event of type CCI – a CCF event that is at the same time an initiator and a loss of a needed safety system. The code gives information about an event with direct interrelations between the accident mitigation systems through common support systems. An event of interest for e.g. PSA analysts, regulators.
Safety culture **(10)**	The cause of the event is in safety culture management. Understanding, communication and management of requirements have failed. The code gives information about CCF events that have occurred that can be attributed as originating from the management and safety culture factors
Multi-Unit CCF (11)	CCF affecting a number of reactors or multiple units at one site The code gives information about CCF events that have occurred and affected several plants at a site. The events have to originate from a common event cause.
No code applicable (12)	Indicates that the event has been analysed but is not considered to be highlighted and therefore none of the codes are applicable.
Other remarkable events (13)	Other remarkable events not covered by the other codes but worth noting. The code gives information e.g. about an important new CCF mechanism, not earlier documented in the licensing documentation or operating history, or about a CCF event that has led to or will lead to a major plant or system modification.
Questionable coding (14)	Indicates that there are comments on the event coding in the analyst comment field.
Shutdown and Decommissioning (15)	Events of special interest for plants planning for permanent shutdown or decommissioning state. This code indicates events where CCF-phenomena were observed which might be of special interest for non-power operation modes. It should not be used for components like the EDGs where the importance in all plant states is obvious.

Annex D – Workshop form

The workshop form included the following questions to answer:

1. Topical question: What type of intersystem dependency impairment (severity) was observed in the event(s)? Choose one of the alternatives below.

   A. Actual intersystem impairment: Failures affecting multiple systems, with strong intersystem dependency. If so, does the latency time overlap between the events?

   B. Partial/Incipient intersystem impairment: Failures/impairment in one system and other system(s) were affected by a similar problem (failure mechanism), e.g. same sub-component.

   C. Potential intersystem impairment: Failures in one system only, but other system(s) could have been affected due to the nature of the failure mechanism.

2. Topical question: Identify the "simultaneity" (time factor) of the intersystem events by determining the time frame between detection of the intersystem events.
3. Topical question: What type of intersystem dependency factor (shared cause) was observed in the event(s)? Select one or more categories from Table D.1.
4. Indicate the most significant factor.
5. Describe the failure mechanism, including the cause of failure, in a few words. For example: "Vibration due to deficient installation led to cracks in fuel pipes."
6. Add the failure mechanism category and sub-category, and the failure cause category.
7. Specify the plant state(s) (in operation, revision etc.) when the event(s) was(were) detected.

For question 7 or 8: Assign the actual or possible defences or improvements to the following categories.

   a) Design of system or site

   b) Design of component

   c) Surveillance of component or maintenance procedure for component

   d) Testing procedure

   e) Operation procedure for component

   f) Management system of plant (QA of the vendor, spare parts management, training of personnel, sufficient resources/staff etc.)

7. If not complete CCF: Can you identify any actual defences that prevented all components from failing?

8. 8-1) If complete CCF: Can you identify any possible defences that could have prevented all components from failing? 8-2) For other events: Can you identify any areas of improvement in order to prevent the event from happening again?
9. If the event is of special interest to others, mark the event with applicable “event category(s)”.

Table D.1. Examples of internal and external factors (other factors could exist)

Intersystem dependency events				
Internal factors with intersystem effects			***External factors with intersystem effects***	
1. Organisational	***2. Human***	***3. Identical components***	***4. Proximity***	***5. Shared SSCs***
a) Incorrect procedure	*Pre-initiator*	a) Same design	a) Area event	a) Connected systems, structures and components
b) Latent design issue	a) Missing surveillances	b) Same operation	b) External event	b) Cooling
c) Incorrect calculation	b) Maintenance cleaning	c) Operating environment	c) Site layout	c) Ventilation
d) Incorrect technical specifications	c) Identical installations	d) Same installation	d) Conduits and doors (may connect otherwise independent areas)	d) Signals
e) Incorrect vendor guidance	d) Transposition errors	e) Maintained nearly identically		e) Common parts
f) Incorrect engineering judgement	e) Identical maintenance actions			
g) A misinterpretation of guidance or requirements	*Post-initiating*			
h) A misunderstanding of system configuration or function	f) Misalignment of breakers after the loss of off-site power (LOOP) or station blackout (SBO)			