Nuclear Safety
NEA/CSNI/R(2019)5
November 2022
www.oecd-nea.org

CDE Topical Report

Provision Against Common-cause Failures by Improving Testing

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CSNI/R(2019)5

Unclassified **English text only**

2 November 2022

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

ICDE Topical Report

Provision Against Common-cause Failures by Improving Testing

This document is available in PDF format only.

JT03506433

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 38 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, Colombia, Costa Rica, 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, Türkiye, 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 34 countries: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia (suspended), the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, 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) addresses 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, several Nuclear Energy Agency (NEA) member countries initiated the International Common-cause Failure Data Exchange (ICDE) Project in 1994. In 1997, the NEA Committee on the Safety of Nuclear Installations (CSNI) formally approved the carrying out of this project within the NEA framework. Since then, the project has successfully operated over six consecutive terms (the seventh term being 2015-2018).

The purpose of the ICDE project is to allow multiple countries to collaborate and exchange common-cause failure (CCF) data to enhance the quality of risk analyses that include CCF modelling. Because CCF events are typically rare events, most countries do not experience enough CCF events to perform meaningful analyses. Data combined from several countries, however, is sufficient for more rigorous analyses.

The objectives of the ICDE project are to:

- collect and analyse common-cause failure (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 that can then be used to derive approaches or mechanisms for their prevention or for mitigating 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 the quantification of CCF frequencies in member countries; and
- 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 probabilistic safety assessment (PSA) or probabilistic risk assessment (PRA) reviews and application.

The ICDE project has produced the following reports, which can be accessed through the NEA website (www.oecd-nea.org):

- Collection and Analysis of Common-cause Failures of Centrifugal Pumps [NEA/CSNI/R(99)2], September 1999.
- Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators [NEA/CSNI/R(2000)20], May 2000.
- Collection and Analysis of Common-Cause Failures 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 the ICDE Workshop on Qualitative and Quantitative Use of ICDE Data [NEA/CSNI/R(2001)8], June 2001.
- Collection and Analysis of Common-Cause Failure of Check Valves [NEA/CSNI/R(2003)15], May 2003.
- Collection and Analysis of Common-Cause Failures of Batteries [NEA/CSNI/R(2003)19], September 2003.
- ICDE Project: General Coding Guidelines – Technical Note [NEA/CSNI/R(2004)4], January 2004.
- Collection and Analysis of Common-Cause Failures of Switching Devices and Circuit Breakers [NEA/CSNI/R(2008)1], October 2007.
- Collection and Analysis of Common-Cause Failures of Level Measurement Components [NEA/CSNI/R(2008)8], March 2008.
- ICDE Project: General Coding Guidelines – Updated Version, [NEA/CSNI/R(2011)12], October 2011.
- Collection and Analysis of Common-Cause Failures of Centrifugal Pumps [NEA/CSNI/R(2013)2], October 2012.
- Collection and Analysis of Common-Cause Failures of Control Rod Drive Assemblies [NEA/CSNI/R(2013)4], July 2013.
- Collection and Analysis of Common-Cause Failures 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 Learned 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], March 2020.
- ICDE Topical report: Provision against Common-Cause Failures by Improving Testing [NEA/CSNI/R(2019)5] (this report).
- ICDE Topical report: Collection and Analysis of Multi-Unit Common-Cause Failure Events [NEA/CSNI/R(2019)6] (forthcoming).

Acknowledgements

The following individuals have contributed significantly to the preparation of this report: Mr Gunnar Johanson (ÅF Pöyry), Mr Mattias Håkansson (ÅF Pöyry), Mr Benjamin Brück (GRS) and Mr Gennadi Loskoutov (SSM).

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. Mr Olli Nevander and Dr Diego Escrig Forano were the administrative NEA officers and contributed to finalising the report.

Table of contents

List of figures

List of tables

Executive summary

This report presents a study performed on a set of common-cause failure (CCF) events within the Nuclear Energy Agency (NEA) International Common-cause Failure Data Exchange (ICDE) Project. The topic was *improving testing*.

The main objective of this topical report 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 broaden their understanding on reducing CCF risks by improving testing and to provide insight into 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 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; quality assurance (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 to improve testing events are:

- A process for quality assurance of procedures to ensure completeness, adequacy and validity of the 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 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 the occurrence of CCFs.

- The defences that prevented events from becoming complete CCFs show that experience feedback from other units and previous similar events can help detect latent failures in time, even when ordinary testing does not identify the failure mechanism.

The two reports "Provision against Common-Cause Failures by Improving Testing" [NEA/CSNI/R(2019)5] (this report) and "Collection and Analysis of Multi-Unit Common-Cause Failure Events" [NEA/CSNI/R(2019)6] (forthcoming) are complementary with a different focus. After publication, it could be of great interest to perform a thorough analysis to connect these findings and conclusions across all of the reports in a next step of the project.

List of abbreviations and acronyms

AFW	Auxiliary feed water
ANVS	Autoriteit Nucleaire Veiligheid en Stralingsbescherming (Netherlands)
CA	Corrective action
CCCG	Common-cause component groups
CCF	Common-cause failure
CF	Coupling factor
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee on the Safety of Nuclear Installations
CVCS	Chemical and volume control system
DE	Demand event
EC	Event cause
EDG	Emergency diesel generator
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat (Switzerland)
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
I&C	Instrumentation and control
ICDE	International Common-cause Failure Data Exchange
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (France)
KAERI	Korea Atomic Energy Research Institute (Korea)
LM	Level measurement
LOCA	Loss of coolant accident
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
QA	Quality assurance
PRA	Probabilistic risk assessment

PSA	Probabilistic safety assessment
SG	Steam generator
SRV	Safety and relief valves
SSM	Swedish Radiation Safety Authority (Sweden)
STUK	Radiation and Nuclear Safety Authority (Finland)
TSO	Technical support organisation
UJV	Nuclear Research Institute (Czech Republic)

NB: The acronyms from the ICDE general coding guideline (NEA, 2011) are presented in Annex 1.C.

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.

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

Corrective action: 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: how the exposed components were detected.

Failure mechanism: 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 1.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.

Incipient failure: the component is capable of performing the safety function, but parts of it are in a state that – if not corrected – would lead to a degraded state. For example, a pump-packing leak that does not prevent the pump from performing its function but could develop to a significant leak.

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.

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.

Shared cause factor: allows the analyst to express his degree of confidence about the multiple impairments resulting from the same cause.

Time factor: a measure of the "simultaneity" of multiple impairments. This can be viewed as an indication of the strength-of-coupling in synchronising failure times.

1. Introduction

One of the main ICDE project objectives is to generate qualitative insights into the causes of CCF events that can be used to improve prevention. The main objective of this topical report is 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. This report summarises the workshop results and presents measures to protect against CCFs by improving testing.

The objectives of this report are:

- to describe the data profile of the ICDE events related to improving testing;
- to develop qualitative insight into the events, expressed by event causes, coupling factors, corrective actions;
- to identify the inadequacies in the testing;
- to identify areas of improvement and possible/actual preventions against such events happening again;
- to recommend provisions against CCFs by improving testing.

Section 2 presents the identification process of events. Section 3 is an overview of the included events with their event parameters. Section 4 contains the engineering insights into the CCF events, supported by the failure mechanism descriptions. These insights are based on the identified inadequacies in testing. Section 5 provides a summary and conclusions. References are found in the dedicated reference section.

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 1.A. Annex 1.B and Annex 1.C lays out the definition of common-cause failures and the ICDE event definitions. Annex 1.D lays out the decision matrix for the CCF root cause analysis. Annex 1.E presents the workshop form that was used in the event analysis.

2. Identification of events

The selection of events related to "improving testing/test procedures" was based on detection mode, latent time of impairment, and applicable events based on event search. The following criteria were used to identify topical events related to improving tests:

- detection mode with latent time longer than the test interval:
  - unscheduled test (TU);
  - maintenance/test (MA);
  - demand event (DE) or test during annual overhaul (TA)[1];
  - test in laboratory (TL);
- event cause as procedure inadequacy (P) with corrective action:
  - general administrative/procedure controls (A);
  - test and maintenance policies (F);
- event search:
  - suggestions from the countries (ICDE members);
  - analyst comments field containing the word "test";
  - events with all components in a group degraded with max one component as completely failed (C) and no components as working (W) and:
    - event cause not coded as D, I, or A;
    - event description (C5) including "test".

In total, the event set includes 71 events (out of about 1 800 ICDE events). However, some events were assessed during the workshop as not applicable to the topic for the workshops[2]. After excluding these, a total of 59 events were included in the statistics.

1. Latent time longer than the test interval and latent time longer than two years (730 days).
2. After the analysis, it was concluded that five events were to be excluded from the statistics as they were assessed as having adequate testing. Seven events were assessed as plant commissioning errors and did not fit the workshop scope. They were excluded from the statistics but are discussed in Section 4.8.

3. Overview of database content

This chapter presents an overview of the data set, which includes 59 events. Tables exhibiting the event count for each event parameter (component type, event cause, coupling factor, corrective action, CCF root cause, detection method and event severity) are presented. The event parameters are defined in the ICDE general coding guidelines (NEA, 2011), see Annex 1.C.

To put the percentages in context for the following tables, two values are given:

- "Percentage" 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.

3.1 Component type and event severity

Table 3.1 and Figure 3.1 present the scope of the workshop and the distribution of the event severity.[3] The most common component types are diesels, centrifugal pumps and safety relief valves, which corresponds quite well to event counts in the total database. Also, the events cover the whole event severity scale, from complete CCF to incipient impairment. The most common event severities are "complete impairment" (51%), "CCF impaired" (19%) and "complete CCF" (14%). The share of "complete CCFs" and "complete

3. *a) 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).

   b) 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).

   c) 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).

   d) 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).

   e) *Incipient impairment* = At least two components in the group are affected, no complete failures and not a complete impairment. At least one component is working.

   f) *Single impairment* = One component affected in the group, but event reported since it includes interesting CCF aspects.

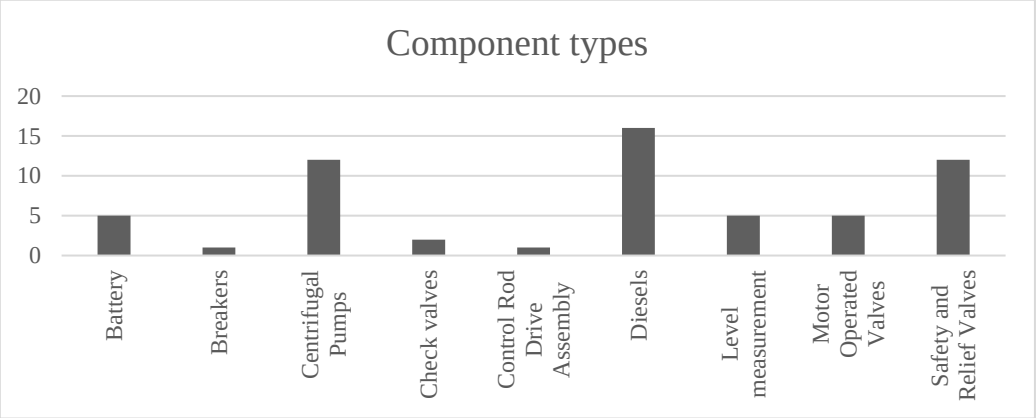
   g) *No impairment* = All components are working but event reported since it includes interesting CCF aspects.

impairment" events are higher compared to the total database, in which about 9% are complete CCFs and 30% are complete impairments.

Table 3.1. The scope of the workshop; distribution of component types per event severity

	Event severity									
Component type	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	No impairment	**Total**	**Percentage**	**Relative Occurrence**
Battery				4	1			5	8%	200%
Breakers					1			1	2%	30%
Centrifugal Pumps				9	3			12	20%	90%
Check valves				2				2	3%	50%
Control Rod Drive Assembly							1	1	2%	20%
Diesels	4		7	4		1		16	27%	210%
Level measurement	3		1	1				5	8%	100%
Motor Operated Valves	1		2	2				5	8%	90%
Safety and Relief Valves		2	1	8	1			12	20%	140%
Total	**8**	**2**	**11**	**30**	**6**	**1**	**1**	**59**	**100%**	
Percentage	**14%**	**3%**	**19%**	**51%**	**10%**	**2%**	**2%**	**100%**		
Relative Occurrence	**150%**	**20%**	**60%**	**260%**	**40%**	**90%**	**-**			

Figure 3.1. Distribution of component types



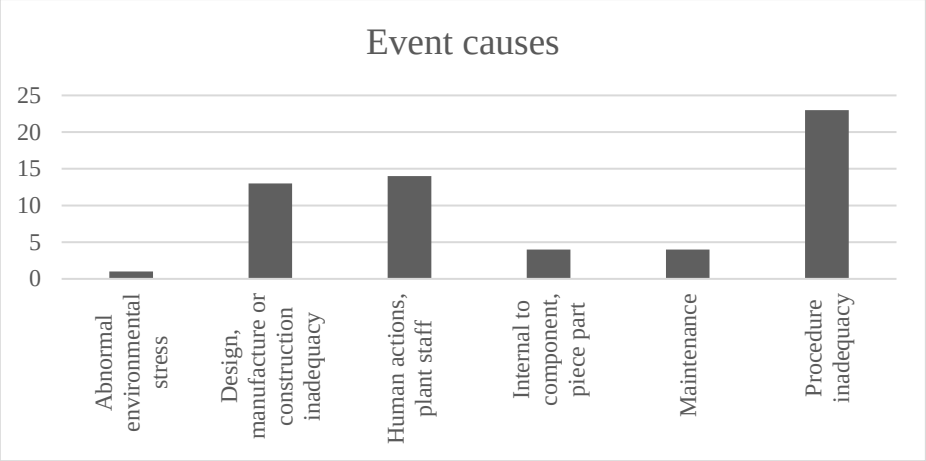
3.2 Event cause (apparent cause)

Table 3.2 and Figure 3.2 present the distribution of the apparent event causes. "Procedure inadequacy" followed by "design, manufacturer and construction inadequacies" and "human actions, plant staff errors" are the most common event causes.

Table 3.2. Distribution of event causes per severity category

Event cause	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	No impairment	**Total**	**Percentage**	**Relative Occurrence**
Abnormal environmental stress	1							1	2%	40%
Design, manufacture or construction inadequacy			2	7	4			13	22%	70%
Human actions, plant staff	2	1	3	5	1	1	1	14	24%	250%
Internal to component, piece part	1		2	1				4	7%	30%
Maintenance			1	3				4	7%	140%
Procedure inadequacy	4	1	3	14	1			23	39%	300%
Total	**8**	**2**	**11**	**30**	**6**	**1**	**1**	**59**	**100%**	

Figure 3.2. Distribution of event causes



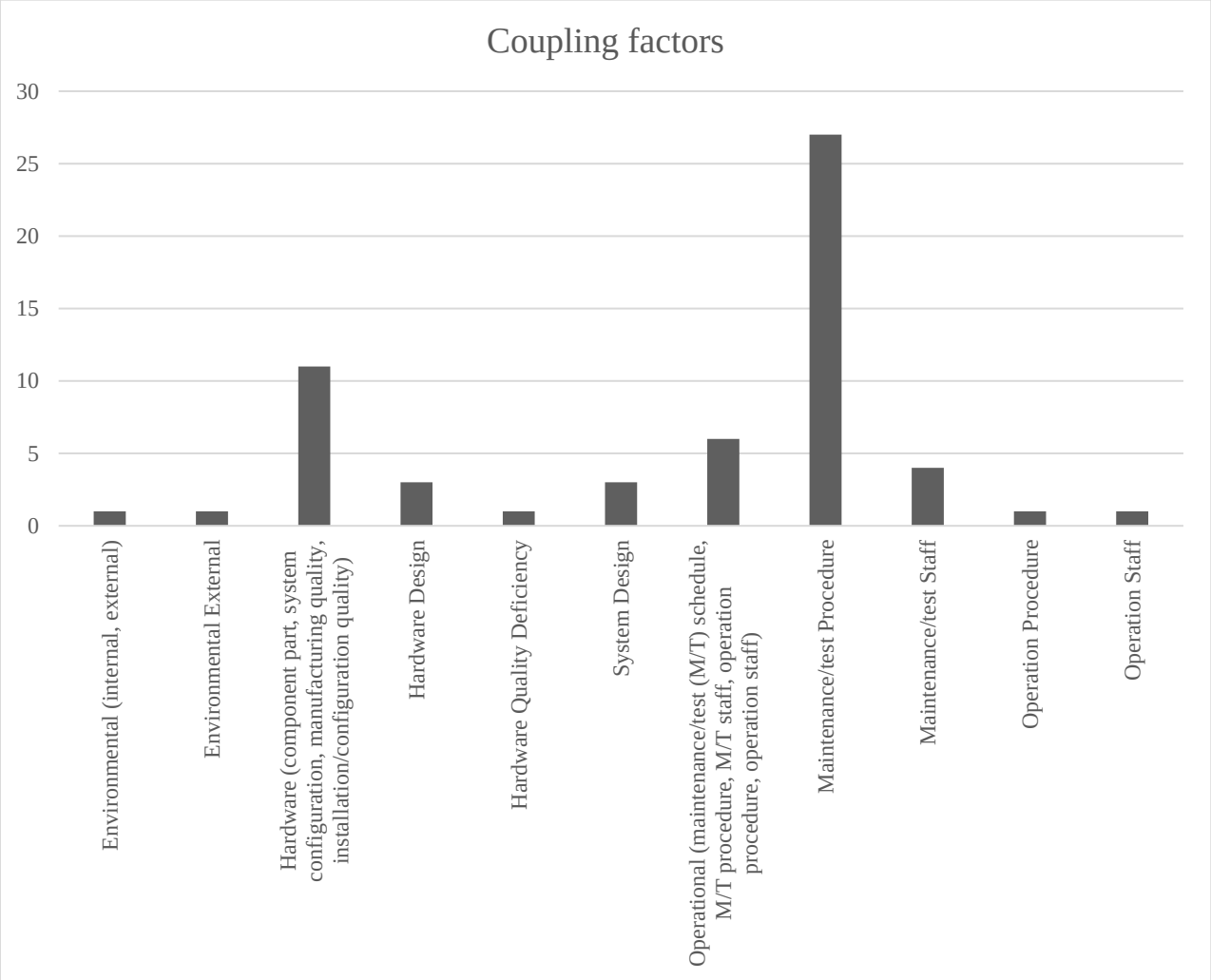
3.3 Coupling factor

Table 3.3 and Figure 3.3 show the distribution of the events by coupling factor. The coupling factor “operational” is most common factor, and about two-thirds of the events are coupled by operational aspects.

Table 3.3. Distribution of coupling factors per severity category

	Event severity									
Coupling factor	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	No impairment	**Total**	**Percentage**	**Relative Occurrence**
Environmental	**1**		**1**					**2**	**3%**	30%
Environmental (internal, external)			1					1	2%	70%
Environmental External	1							1	2%	80%
Hardware	**2**		**3**	**9**	**3**		**1**	**18**	**31%**	**60%**
Hardware (component part, system configuration, manufacturing quality, installation/configuration quality)	2		2	4	2		1	11	19%	100%
Hardware Design			1	2				3	5%	30%
Hardware Quality Deficiency				1				1	2%	50%
System Design				2	1			3	5%	70%
Operational	**5**	**2**	**7**	**21**	**3**	**1**		**39**	**66%**	**170%**
Maintenance/test Procedure	4	2	3	17	1			27	46%	340%
Maintenance/test Staff			1	1	2			4	7%	140%
Operational (maintenance/test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)			3	3				6	10%	120%
Operation Procedure	1							1	2%	120%
Operation Staff						1		1	2%	260%
Total	**8**	**2**	**11**	**30**	**6**	**1**	**1**	**59**	**100%**	

Figure 3.3. Distribution of coupling factors



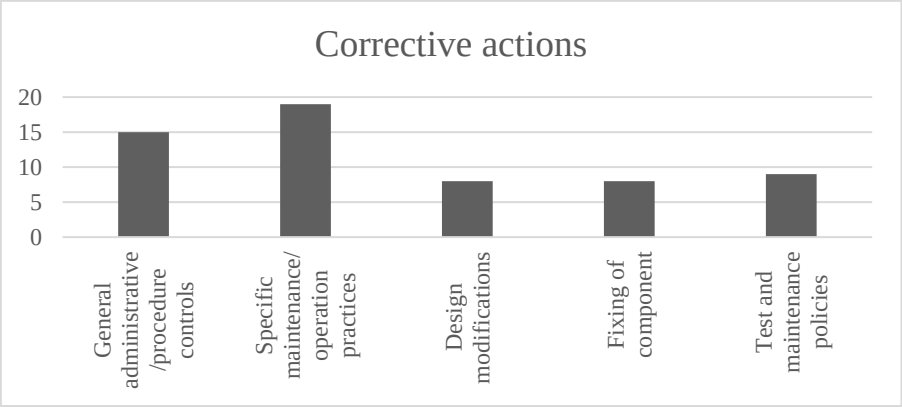
3.4 Corrective action

Table 3.4 and Figure 3.4 show the distribution of the events by corrective action. The most common corrective actions are “specific maintenance/operation practices” and “general administrative/procedure control”.

Table 3.4. Distribution of corrective actions per severity category

	Event severity									
Corrective action	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	No impairment	**Total**	**Percentage**	**Relative Occurrence**
General administrative/ procedure controls	3	1	2	6	1	1	1	15	25%	170%
Specific maintenance/ operation practices	1		5	12	1			19	32%	130%
Design modifications			3	4	1			8	14%	60%
Fixing of component	2		1	2	3			8	14%	100%
Test and maintenance policies	2	1		6				9	15%	140%
Total	**8**	**2**	**11**	**30**	**6**	**1**	**1**	**59**	**100%**	

Figure 3.4. Distribution of corrective actions



The root cause is "the most fundamental reason for an event or adverse condition, which if corrected will effectively prevent or minimise recurrence of the event or condition."[4] By combining the coded information for the (apparent) event cause (EC) and the corrective action (CA) and the coupling factor (CF), insights regarding the CCF root cause of the test inadequacy events can be gained. Each of these three provides one root cause aspect, 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).

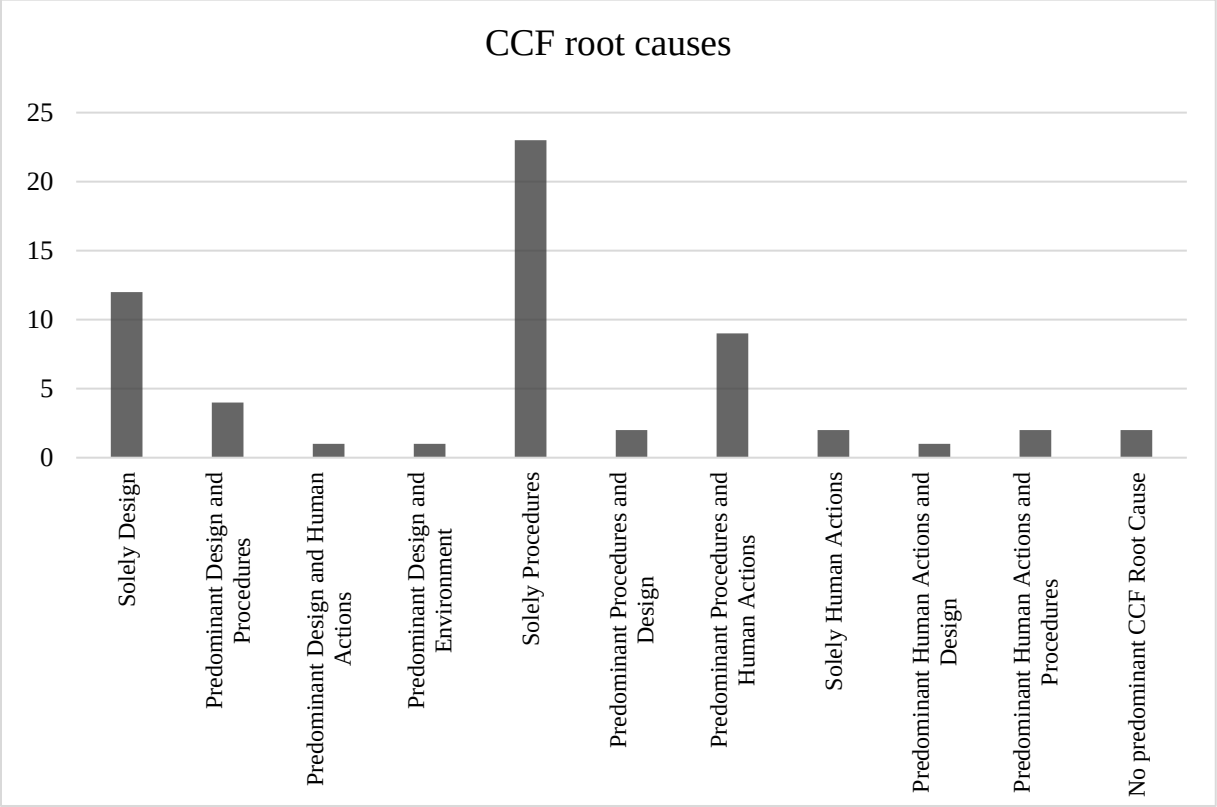
4. See IAEA-TECDOC-1 756 for more details

In addition to these three basic aspects, the supporting aspects "environmental" and "unknown" are used for case events due to external factors or events which 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 Annex 1.D. The results of the CCF root cause assignment are given in Table 3.5 and Figure 3.5.

Table 3.5. 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	No Impairment	**Total**	**Percentage**
Solely or predominantly design	**2**		**4**	**9**	**3**			**18**	**31%**
Solely Design	1		3	6	2			12	20%
Predominant Design and Procedures				3	1			4	7%
Predominant Design and Human Actions	1							1	2%
Predominant Design and Environment			1					1	2%
Solely or predominantly procedures	**5**	**2**	**6**	**20**	**1**			**34**	**58%**
Solely Procedures	4	1	4	14				23	39%
Predominant Procedures and Design				2				2	3%
Predominant Procedures and Human Actions	1	1	2	4	1			9	15%
Solely or predominantly human actions			**1**	**1**	**2**	**1**		**5**	**8%**
Solely Human Actions			1	1				2	3%
Predominant Human Actions and Design					1			1	2%
Predominant Human Actions and Procedures					1	1		2	3%
No predominant CCF Root Cause	**1**						**1**	**2**	**3%**
Total	**8**	**2**	**11**	**30**	**6**	**1**	**1**	**59**	**100%**

Figure 3.5. Distribution of CCF root causes



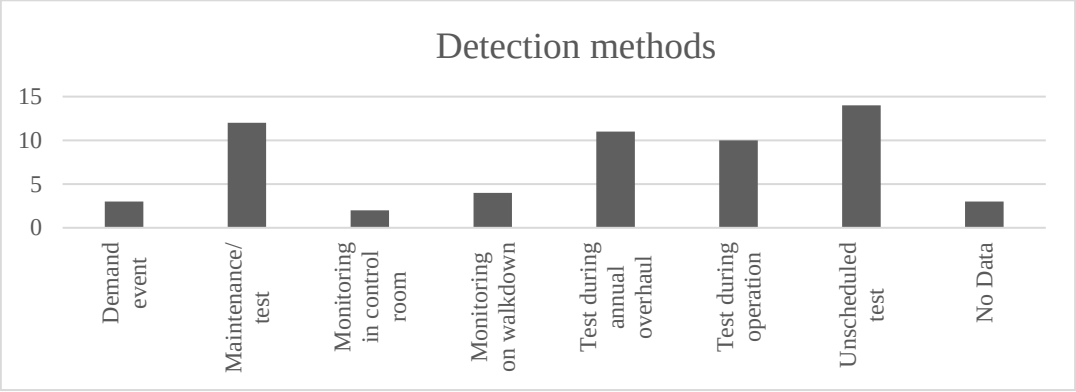
3.5 Detection method

Table 3.6 and Figure 3.6 show the distribution of the events by detection method. The detection methods are distributed mainly over four different methods but no specific detection method is particularly common and only three events are “demand events”.

Table 3.6. Distribution of detection methods per severity category

	Event severity								
Detection method	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	Single impairment	No impairment	**Total**	**Percentage**
Demand event	1	1	1					3	5%
Maintenance/test	1	1	3	6	1			12	20%
Monitoring in control room			1	1				2	3%
Monitoring on walkdown				4				4	7%
Test during annual overhaul	3			6	1		1	11	19%
Test during operation	1		3	5		1		10	17%
Unscheduled test	2		1	7	4			14	24%
No Data			2	1				3	5%
Total	**8**	**2**	**11**	**30**	**6**	**1**	**1**	**59**	**100%**

Figure 3.6. Distribution of detection methods



4. Engineering aspects of the collected events

This chapter presents the engineering aspects of the analysed events. The analysis was performed according to the workshop form in Annex 1.E. Workshop form. After the analysis, it was concluded that five events be excluded from the statistics, as they were assessed to have had adequate testing. Seven events were assessed as plant commissioning errors and did not fit the workshop scope. They were excluded from the statistics but are discussed in Section 4.8. A total of 59 events are therefore included in the statistics in the following sections.

4.1 Assessment basis

The engineering aspects of the event analysis comprised:

- What happened?
  - observed inadequacies in testing;
  - plant state when the event was detected;
  - failure mechanism descriptions.
- What can be done to prevent this from happening again?
  - prevention – CCF defence aspects;
  - areas of improvement;
  - interesting events – discussion and examples;
  - plant commissioning error events.

Failure mechanism description

The failure mechanism is 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. It is derived from the event description and should preferably consist of one sentence. The failure mechanism descriptions for the events are presented in Sections 4.2 and 4.8.

Test inadequacy category

Based on the observed inadequacies in the testing, test inadequacy categories and sub-categories have been developed. A test inadequacy category is a group of similar testing inadequacies categorising the factors that led to the ICDE event.

An event could be assigned to more than one category, i.e. the categories are not exclusive. Table 4.1 presents the test inadequacy categories and sub-categories.

Table 4.1. Test inadequacy categories and sub-categories

Test inadequacy category and sub-category	
A. Extent of the test	1. Not all operating modes (power operation, during start-up, long term outage, etc.) covered by the test scope 2. Not all operating conditions (e.g. emergency conditions) covered by the test scope 3. Not all aspects on system level covered by the test scope
B. QA of test/maintenance/modification	1. Inadequate process to ensure completeness of test 2. Inadequate process to ensure adequacy of test 3. Inadequate process to ensure validity of test 4. Inadequate update of procedures after modification
C. Performing the test	1. Inadequate instructions/checklists 2. Inadequate use of equipment/instruments (e.g. not calibrated) 3. Inadequate training of staff 4. Omission of procedure step
D. Verification of operability	1. Verification of operability after test 2. Verification of operability after maintenance 3. Verification of operability after modification

Plant state when the event was detected

Part of the event analysis is to identify the plant's state when the event was detected. This information can provide a sense of severity to 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 so). This aspect is often 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 that prevented failure of all components in the group. In other cases, it may only be by accident or luck that all the components did not fail.

Areas of improvement

The areas of improvement identifies what could prevent the event from happening again, can be considered as lessons learnt from the event analysis, and identifies possible defences to prevent 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. Several areas may be relevant for a single event.

Marking of interesting events

Marking interesting events in the ICDE database consists of pointing out interesting and extra ordinary CCF event records such as subtle dependencies with specific codes and descriptions. These records are important dependency events that are useful for the overall operating experience and can also be used as input for the stakeholders to develop defences against CCFs. Several areas may be relevant for a single event.

4.2 Inadequacies in testing

The initial step in the analysis was to identify the inadequacy in the testing that led to the event according to the categories introduced in Section 4.1. The results are shown in Table 4.2. An event could be assigned to more than one category. Each category has sub-categories to further specify the observed problems.

Table 4.2. Inadequacies in testing

Test inadequacy	Total
A. Extent of test	16
B. QA of test/maintenance/modification	33
C. Performance of test	9
D. Verification of operability	18
Unknown	2

The following sub-sections present the events for each category together with the failure mechanism description, which describes the observed event and influences leading to the given failure, and possible improvements to prevent the event from happening again.

4.2.1 Extent of test

A total of 16 events were assigned to this category. Three events concerned operating modes and two events concerned operating conditions, categories A1 and A2, respectively. These test inadequacies should be interpreted as issues on the plant level. A total of 11 events concerned the system test scope, category A3. This category indicates that the testing did not cover all aspects on the system level to prevent the event from happening.

A1 All operating modes

Failure mechanism description	Improvement
– During an audit, the battery system was found incapable of meeting its capacity requirements for some operating modes (certain system tests during power operation). No tests were performed that could have revealed this deficiency, so the inadequate capacity remained undetected for over 24 years.	➢ Testing procedures (tests to be performed during all operating modes). Process to ensure completeness of tests.
– The battery bank consisting of two batteries was not capable of supplying required loads due to insufficient capacity (system design error).	➢ Design of system. An appropriate testing procedure did not exist. The utility should have developed a procedure to confirm that a single battery bank would supply the required loads.
– Complete CCF, see Section 4.4.	

A2 All operating conditions

Failure mechanism description	Improvement
– Higher (valve disc) friction factor than expected led to the failure of a MOV and a degraded safety margin for other MOVs. It was determined that the capability of the valves to work under emergency operating conditions (higher differential pressure over the valve than during normal operation) was not ensured.	➢ Design of component. Testing procedure (not possible to test under emergency conditions). All test and maintenance activities should be certified even for emergency conditions. Laboratory test with emergency conditions would have prevented the event.
– Manufacturer staff used unsuited grease when making a modification of MOVs, leading to a potential CCF failure of valves during an accident situation when the temperatures at the valves are much higher than during normal operation and testing. The regular testing programme was not able to identify the unsuitable grease.	➢ Management system - better training and surveillance of manufacturer staff (should be aware of the importance of specifications for grease).

A3 Testing scope

Failure mechanism description	Improvement
– A pilot valve failed to open due to adhesive coating on the valve actuator. The unscheduled test was carried out after an event in another plant. Similar coatings were found on other valves but no failures were observed.	➢ The test interval (one year) was too long to detect the failure mechanism in time. The testing procedure should be improved to check that the actuator is functional.
– In case of short circuit, the fault current may destroy the switchgear because the two new batteries led to a higher short circuit current than it was designed for.	➢ Adequate design of the switch gear and testing after the modification.
– Following a modification on both trains A and B, the breaking and the omission of the locking device of the check valves resulted in failure to remain close.	➢ Design of component, maintenance procedure. A backflow testing on train A would have prevented all components to fail (train B).
– At a full scope test it was discovered that the maximum pump design flow could not be achieved at times of high demand. This was caused by incorrect leak-off valve settings that resulted in water passing from pump discharge around the recirculation route. The inadequate settings persisted undetected for 14 years and affected both pumps.	➢ The testing procedure was changed to check the leak-off valves settings routinely.
– The battery bank consisting of three batteries was not capable of supplying required loads due to insufficient capacity, i.e. undersized batteries (system design error).	➢ Design of system. The testing shall ensure that the required capacity is verified.

4.2.2 QA of test/maintenance/modification

Table 4.3 shows how the events in this category were distributed. Quality assurance (QA) of completeness and adequacy of testing were the most common issues.

Table 4.3. Test inadequacy - QA of test/maintenance/modification

Test inadequacy	Total
B. QA of test/maintenance/modification	**33**
B1. Completeness	12
B2. Adequacy	13
B3. Validity	4
B4. Update process after modification	4

B1 Completeness of test/maintenance/modification

Failure mechanism description	Improvement
– Filters used in cleaning operations at the auxiliary feed water (AFW) pumps were not removed at the end of the cleaning operation. There was no performance degradation of the pumps as long as they were operated with clean demineralised water, but in case raw water was used during an emergency situation, the filters would have clogged.	➢ Add a step in the maintenance procedure for removal of temporary filter.
– Hand valves erroneously not reopened after a maintenance inspection led to the isolation of all pilot lines of one of the main safety valves station and then to a steam generator (SG) without protection against overpressure. No adequate testing was performed before start-up of the unit to ensure the correct position of the valves.	➢ General administrative/procedure control.
– The opening time of the SRVs exceeded the Tech Spec requirement which was not specified in the test procedure.	➢ Verification of testing procedure.
– The procedures did not include a step to perturb (i.e. braise and then lower) the reactor water level following instrument calibration. Without perturbing the level, a frozen measurement could not be detected with certainty.	➢ Revision of testing procedure.

B2 Adequacy of test/maintenance/modification

Failure mechanism description	Improvement
– Because of the testing method used, the batteries were discharged beyond recommended levels, which shortened their expected life.	➢ Improve the discharge test procedure.

B2 Adequacy of test/maintenance/modification

Failure mechanism description	Improvement
– Locking of automatic start-up of both EDGs was erroneously required by the test procedure on another component.	➢ Better QA of test procedures would have prevented the event from happening.
– The valve alignments established by the procedure could, for a brief period of time, render both pumps potentially inoperable.	➢ Provide test personnel with a caution statement specifying required actions should a system initiation occur.

B3 Validity of test/maintenance/modification

Failure mechanism description	Improvement
– A design with overly small orifices in the flow meters limited the flow rate of the emergency feed water pumps.	➢ Design of component. Process to ensure completeness, quality and validity of tests.
– Confusion between pressure units led to the SRV settings not complying with operating specifications.	➢ Management system of plant (training of staff, verification of implementation of commitments). Process to ensure completeness, quality and validity of tests.
– Inadequate test procedure resulted in damage to the air start distributer and the EDGs failed to start.	➢ Improvement of test procedure by not requiring air to be applied to the distributor while running the diesel during the test.
– Maintenance instructions were not updated, which resulted in wrong settings of the opening pressure of two SRVs. Also, the test method was not sufficiently accurate to comply with the operating rules.	➢ Process to ensure completeness, quality and validity of tests (consistency between operating rules and maintenance tests). The accuracy of the test may have been avoided with a check of calibration instruments.

B4 Update process after modification

Failure mechanism description	Improvement
– Pump seal failure due to faulty maintenance. The pump mechanical seal had been installed improperly during the last outage. The quarterly surveillance test identified the problem before any demand occurred, which could have led to failure of both pumps.	➢ Improve post-maintenance test and improve maintenance procedure.
– When backfitting additional (diverse) motor operated safety valves not all possible accident conditions were taken into account. This would have led to an incomplete opening of these valves in some accident situations.	➢ Design of component.

B4 Update process after modification

Failure mechanism description	Improvement
– Two Complete CCF, see Section 4.4.	

4.2.3 Performing the test

Nine events were assigned to the category "performing the test", which identifies the types of errors that can be related to performing the test. It focuses on instructions, use of equipment, training of staff and work control (use of written procedure).

C1 Instructions/Checklists

Failure mechanism description	Improvement
– Incorrect assembled coupling between pump and motor, which would have failed in case of disassembling. This was not detected during the previous periodic tests.	➢ Better QA of the test procedure.
– Incorrect setting of the operating mode after test led to wrong operating mode of one of the four level transmitters.	➢ Include in the verification of operability a step to check the operating mode of the transmitters after testing.

C2 Use of equipment/instruments

Failure mechanism description	Improvement
– A wrong scaling factor in the equipment for testing the set points of steam generator safety valves led to setting the set points of the SRVs too low. This was only detected when the testing equipment was replaced by a new one with a new testing method.	➢ Testing procedure for component. Use different equipment for setting set points for safety valves.
– Opening pressure for the SRVs was set too high due to inadequate testing method.	➢ The testing equipment and method were inadequate. The testing method was revised.
– Two Complete CCF, see Section 4.4.	

C3 Training of staff

Failure mechanism description	Improvement
– Routine inspection found material, used in non-destructive examinations, in the hydraulic scram system (not detected by optical inspections). However, there was no failure of components (the event is reported to ICDE because the observed CCF phenomenon is interesting).	➢ Better work control. Functional testing.

C4 Omission of procedure step

Failure mechanism description	Improvement
– Both EDGs observed in under-speed condition. The first diesel due to inadequate post-maintenance testing (skipped a test) following replacement of the governor. The second diesel due to incorrectly adjusting the speed control governor.	➢ Safety culture (do not omit steps in the work order). Verification of operability after test and maintenance.

4.2.4 Verification of operability

A total of 18 events were assigned to the category "verification of operability after test, maintenance or modification". This category focuses on identifying events where the operability is inadequate after activities where latent failures may occur at a real demand. The most common inadequacy was related to verification of operability after maintenance.

D1 Verification of operability after test

Failure mechanism description	Improvement
– Incorrect setting of the operating mode after test led to wrong operating mode of one of the four level transmitters.	➢ Include in the verification of operability a step to check the operating mode of the transmitters after testing.

D2 Verification of operability after maintenance

Failure mechanism description	Improvement
– Fibres probably coming from inappropriate textile absorbent pad used to clean the oil tank, due to an insufficiently precise procedure, led to clogging of filters of the lubrication system to the EDGs.	➢ A special warning and improved verification of cleaning procedures could have prevented the source of clogging.
– The fuel transfer pump valves were in the wrong position after the test, which resulted in an inability to fill the EDG day tanks.	➢ Verification of operability after test. The test procedure was updated with a check of the valve position.

D2 Verification of operability after maintenance

Failure mechanism description	Improvement
– The EDG connector was incorrectly re-assembled during maintenance, which led to two phases being reversed, causing a wrong spark sequences from the exciter. This was not detected because of incomplete testing after maintenance.	➢ Verification of operability after maintenance. Skipped important test after overhaul.

D3 Verification of operability after modification

Failure mechanism description	Improvement
– When replacing the breaker timing relays with relays from a different manufacturer it was not recognised that the wiring had to be adapted because the relays were not compatible. This would have led to non-switching of breakers for one specific scenario for restoration of auxiliary power. – Complete CCF, see Section 4.4.	➢ Spare parts management. Make complete system test after modifications.

4.2.5 Unknown test inadequacy

For two events, it was not possible to identify the test inadequacy when assessing the event.

Unknown test inadequacy

Failure mechanism description	Improvement
– Incorrect timing relays were mounted in the three pump motors due to use of wrong relays in store. The condition was discovered during an inspection that was initiated following a fault on an adjacent unit.	➢ Spare parts management.
– Inadequate design may cause the pumps to trip due to a missing interlock in the low voltage protection system. The interlock includes timing elements that avoid unnecessary actuation of the protection system. The design deficiency was detected during a simulator test.	➢ Adequate design of the protection system.

4.3 Plant state when the event was detected

Table 4.4 presents the plant state when the event 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 events occur and whether any trend is observed concerning events with inadequate testing. The most common plant state was power operation, followed by shutdown and outage.

Table 4.4. Plant state when the events were detected

Plant state	Count	Percentage
At power	20	34%
Shutdown	14	24%
Outage	11	19%
Other	3	5%
Unknown	11	19%
Total	**59**	**100%**

4.4 Lessons learnt from complete CCFs

The engineering analysis identified the CCF defences that were present during the events and possible improvements to defences. The defences should be considered ways to keep 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 had completely failed, 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 4.5. Each possible defence is assigned to one of the categories given in the workshop form, as shown in Annex 1.E. Workshop form.

Eight events were complete CCFs. Four complete CCF events involved the component type emergency diesel generators (EDGs):

- An error in the test procedure disabled the automatic start function of all EDGs during a test of the turbine driven emergency power supply. The knowledge and safety awareness of the personnel 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 a lesson learnt, a test of one system may cause problems in another system.
- A test procedure that erroneously required locking of automatic start-up of both EDGs was not corrected due to a lack of monitoring in procedure modifications. The improvements suggested were better checks of the test procedures before implementing them, a better process for updating procedures, and better communication.
- A failure of coupling pins led to loss of fuel supply, preventing both EDGs to start. The failure developed slowly over time. Maintenance of the component was not efficient (ageing problem of the pins). Also, the testing of the component was not efficient. Different test procedures could have detected the pin fatigue earlier. As a corrective action, tests were modified to detect coupling pin failure.
- 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. The use of pressure instrumentation could have prevented the event. Also, verification of operability after maintenance could have been improved.

Three complete CCF events involved the component type level measurement (LM):

- Both level transmitters were replaced without updating the calibration procedure, which meant that 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 could only check the level measurement by simulating a draining of the tank. A functional test with draining of the tank could have prevented the event.

- An erroneous calculation of the theoretical calibration signal, affecting both level limit switches, led to the switches not triggering for the right water level. A check of the calibration instrument after calibration tasks was not performed. After this event, the test procedures were changed so that a faulty indication would be discovered.
- The three level transmitters of the pressuriser did not fulfil their function during emergency conditions due to the fact that 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.

The last complete CCF event involved the component type motor operated valves (MOVs). 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 shutdown phase as required in the technical specifications. The design should have been reviewed and tested for all plant modes, and testing of the modification during plant shutdown should have been performed. Diversity in maintenance teams would increase the possibility of identifying such failures.

4.5 Lessons learnt from actual 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. all components from failing. Each actual defence should be assigned to one of the categories given in the workshop form in Annex 1.E.

For about 34% of the events, no defence that prevented the event from developing into a complete CCF could be identified. This could indicate that most events have a robust design and sufficient procedures for maintenance, test and verification of operability. However, it could also be that the event descriptions are too limited/sparse to be able to identify an actual defence with a high degree of confidence. The results indicate the difficulties of covering the special types of observed failure mechanisms by ordinary designs, procedures, etc.

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

- An event where the pump mechanical seal had been installed improperly during the last outage. The quarterly surveillance test identified the problem before any demand occurred that could have led to failure of both pumps. An insufficient maintenance procedure and inadequate post-maintenance test were identified as factors that led to the event.
- An event where the two pumps' maximum design flow could not be achieved at times of high cooling demand. This was caused by incorrect leak-off valve settings that resulted in water passing from pump discharge around the recirculation route.

The maintenance procedure did not specify the valve settings. A fully instrumented test was performed during a forced outage, which detected the problem.

- An event where incorrect timing relays were mounted in the three pump motors due to the use of wrong relays in store. The condition was discovered during an inspection that had been initiated following a fault in an adjacent unit.

4.6 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 from happening again. There were six areas of improvements to choose from, and an event could be assigned to multiple areas, which affects the event count.

Table 4.5 presents the distribution of testing inadequacies 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 4.2.

4.7 Interesting events – discussion and examples

Table 4.6 presents the statistics per interesting event code. The complete CCF events are presented in Section 4.4.

Table 4.6. Applied interesting event codes

Interesting CCF event codes	**Description** ***Purpose***	**No. of events**
Complete CCF (1)	Event has led to a complete CCF. *This code sums up all complete CCFs, for any component type.*	8
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.*	20
Component not capable (3)	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 would not perform the licensed safety function during the mission time.*	3
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.*	1
Sequence of multiple CCF failure mechanisms (6)	Events with a sequence of multiple CCF failure mechanisms. *The code gives information about incidents which revealed that during the event sequence more than one CCF failure mechanism was observed. The code focuses on the sequence of failures in the observed CCF failure mechanisms, regardless how many common-cause component groups (CCCGs) were affected.*	0
Multiple systems affected (8)	Events where a single CCF failure mechanism affected multiple systems. *This code indicates events where a single CCF failure 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).*	1
Common-cause initiator (9)	A dependency event originating from an initiating event of type common-cause initiator (CCI) – a CCF event which 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.*	0
Safety culture (10)	The reason why the event happened originates from 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.*	10

Table 4.6. Applied interesting event codes (Continued)

Interesting CCF event codes	Description *Purpose*	No. of events
Multi-unit CCF (11)	CCF affecting a fleet 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 root cause.*	19
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.	15
Total		**77**

The insights from the applied interesting event codes are:

- CCF outside planned test: About one-third of the events were assigned to this category. Among the events in this category, events were detected through experience feedback (often from another unit or event), by an unplanned control, in a simulator test, and by an unscheduled test.
- Multi-unit CCF: About 30% of the events were assigned to this category. The type of multi-unit aspects observed include internal shared factors covering human, organisation and common design aspects. One example is an event where filters were left inadvertently on all three centrifugal pumps' suction line intake after maintenance. The cleaning procedure required a filter installation before the cleaning operation but it did not require to remove it at the end of the operation. The periodic tests did not reveal any degradation but in case of clogging of filters, this would have degraded the pumps. This error was observed on three different units at one site.
- Safety culture: About 17% of the events involved inadequacies related to safety culture. One example is an event where all hand valves were erroneously not reopened after a maintenance inspection, which led to the isolation of all pilot lines of one of the four main safety valve stations. Further investigation revealed organisation deficits in the maintenance management of the plant.
- Component not capable: Three events were assessed as not capable to perform their function over a long period of time. One example is an event where the flow meters to the three emergency feed water pumps were designed with orifices that were too small, limiting the flow rate (reported twice the real value) of the pumps. These are used for flow limitation as part of the pumps' component protection. The error was not noticed for 13 years.

4.8 Plant commissioning error events

In the analysis, seven events were assessed to be plant commissioning error events. These events were determined to not fit the scope of the workshop and have been excluded from the above engineering aspects. However, the engineering insights from the analysis of these events are interesting since they show inadequacies of the plant commissioning phase.

For these events, the regular testing identified the issues before the events progressed into complete failures. Thus, the testing procedures were adequate. However, the events show failure causes related to the design, commissioning tests by the manufacturer, and oversight of the manufacturer at the plant commissioning phase.

The insights from these events are:

- An SRV event in which multiple SRVs failed to remain open during test due to leakage of instrument air. The main causes were inadequate safety system test procedures, inadequate installation and inadequate commissioning testing. Adequate systematic testing after installation would have avoided the failures.
- A heat exchanger event in which two heat exchangers failed due to poor quality assurance by the manufacturer (did not perform required tests). Diversity in the manufacturers prevented all four components from failing. Also, non-destructive examination tests identified the weld joint imperfections.
- A diesel event in which fatigue cracks on diesel engine parts (con-rods) was detected by normal maintenance (routine inspection during overhaul). The design was changed on all four diesels after the utility discovered the cracks. As preventive action, the utility should have better oversight of the manufacturer.
- A MOV event in which multiple isolation valves may not open during a large LOCA due to the fact that high differential pressure could exceed the torque switch limit and prevent the valves from opening. The event revealed a misconception of how the system works and how conservative assumptions had been applied. Proper design of the torque switch was suggested as an improvement.
- A level measurement event in which the condensing chambers were not installed per the specifications (wrong connections due to faulty documents) to all six transmitters, resulting in deviations of the level measurement. This level deviation could be large under some LOCA conditions. As actual defence, the design of the system resulted in only a small deviation. Improved verifications after construction and improved mounting instructions could have prevented the event.
- A level measurement event in which both of two level sensors of the containment sump were placed at a wrong position. The problem was discovered after more than 16 years and existed from the commissioning of the plant. Periodic testing could not detect this fault because the test only simulated the draining of the containment sump. Better QA of the test procedure could have prevented the event.
- A level measurement event in which three out of four gauge lines of the level measurements were erroneously interchanged during plant construction. This led to freezing and prevention of the accumulator low level measurement signal. This could not be detected because the accumulators are not emptied during normal testing. By coincidence not all gauge lines were interchanged. Better QA during construction could have prevented the event.

5. Summary and conclusions

The workshop included 59 ICDE events where the testing procedures were inadequate. The goal was to identify testing inadequacies and ways to improve testing to reduce detection times and the risk of such events occurring. In addition to the 59 events, seven events were assessed as plant commissioning errors and were excluded from the general statistics.

Summary of database content:

- The most common component types were EDGs, Centrifugal pumps and SRVs. Level measurement contributed with several severe events.
- "Procedure inadequacy" followed by "design, manufacturer and construction inadequacies" and "human actions, plant staff errors" were the most common event causes.
- The coupling factor "operational" was the most common factor, with about 66% of the events coupled with operational aspects. The environmental coupling factor was rare.
- The most common corrective actions were "specific maintenance/operation practices" and "general administrative/procedure control".
- The most common CCF root cause was "solely and predominantly procedures" (58%), i.e. CCF root cause aspects with deficiencies in procedures.
- No specific detection method was common. The detection methods were distributed mainly over four different methods, and only three events were "demand events".
- The most common event severities were "complete impairment" (51%), "CCF Impaired" (19%) and "complete CCF" (14%). The share of complete CCFs is higher compared to the total database, in which about 10% are complete CCFs.

Table 5.1. Summary of test inadequacy categories and sub-categories

Test inadequacy category and sub-category	Summary
A. Extent of the test 1. Not all operating modes covered by the test scope 2. Not all operating conditions covered by the test scope 3. Not all aspects on system level covered by the test scope	Sixteen events were assigned to this category. Three events concerned operating modes and two events concerned operating conditions. These test inadequacies should be interpreted as issues on the plant level. Eleven events concerned the system test scope. This category indicates that the testing did not cover all aspects on the system level to prevent the event from happening.
B. QA of test/maintenance/modification 1. Process to ensure completeness of test 2. Process to ensure adequacy of test 3. Process to ensure validity of test 4. Update process/procedure after modification	Thirty-three events were assigned to this category, which was the most common. Quality assurance (QA) of completeness and adequacy of testing were the most common issues among the sub-categories.

Table 5.1. Summary of test inadequacy categories and sub-categories (Continued)

Test inadequacy category and sub-category	Summary
C. Performing the test 1. Inadequate instructions/checklists 2. Inadequate use of equipment/instruments 3. Inadequate training of staff 4. Omission of procedure step	Nine events were assigned to this category. This category identifies the types of errors that can be related to performing the test. It focuses on instructions, use of equipment, training of staff and work control (use of written procedure).
D. Verification of operability 1. Verification of operability after test 2. Verification of operability after maintenance 3. Verification of operability after modification	Eighteen events were assigned to this category. This category focuses on identifying events where the operability is inadequate after activities where latent failures may occur at a real demand. The most common inadequacy was related to verification of operability after maintenance.

Summary of the engineering aspects:

- Inadequacies in testing have been observed in all aspects of testing: extent of the test, QA of the test, performance of 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 an inadequate test interval.
- About 34% of the events were detected at power operation.
- Complete CCFs were observed – four diesel events, three level measurement events and one MOV event.
- For about 34% of the events, no actual defence could be identified that would have prevented the event.
- Actual observed defences involve surveillance and inspections, different types of tests (not ordinary tests), defences attributed to the management system of the plant, such as experience feedback from another unit, unplanned control and audit.
- The most common areas of improvement were testing procedure, maintenance procedure and management of plant.
- The marking of interesting events showed that about 30% of the events were detected outside of planned tests. About 30% of the events were marked as multi-unit events and ten events showed deficiencies in safety culture.
- The plant commissioning error events had failure causes related to the design, commissioning tests by the manufacturer, and oversight of the manufacturer at the plant commissioning phase.

The lessons learnt from the engineering aspects analysis are:

- A process for quality assurance of procedures to ensure completeness, adequacy and validity of tests is 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 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 CCFs.
- The actual defences that prevented events from becoming complete CCFs show that experience feedback from other units and previous similar events can help detect latent failures in time, even when ordinary testing does not identify the failure mechanism.

In summary, the engineering aspects include events with test inadequacies covering the extent of test, QA of test, performance of the test, and verification of operability. Several main issues/inadequacies related to tests were observed in the collected events, and defences and improvements were identified. Based on the lessons learnt, several factors/areas of testing need to be considered to improve testing and to create successful defences against CCFs.

References

NEA (2011), "International Common-Cause Failure Data Exchange ICDE General Coding Guidelines – Updated Version", NEA/CSNI/R(2011)12, OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_19122.

Annex 1.A. Overview of the ICDE Project

Background

Common-cause failure (CCF) events can significantly impact the availability of safety systems of nuclear power plants. In recognition of this, CCF data are systematically being collected and analysed in 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 the 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, preparation for the International Common-cause Data Exchange (ICDE) Project began in August 1994. Since April 1998, the NEA has formally operated the project, following which the project was successfully operated over six consecutive terms from 1998 to 2014. The phase that started in 2015 ran until the end of 2018. Member countries under the current Agreement of the NEA and the organisations representing them in the project are: Canada (CNSC), Czech Republic (UJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), Korea (KAERI), Netherlands (ANVS), Spain (CSN), Sweden (SSM), Switzerland (ENSI), and United States (NRC).

More information about the ICDE project can be found on the NEA web site: www.oecd-nea.org/jcms/pl_25090/. Additional information can also be found at the website https://projectportal.afconsult.com/ProjectPortal/icde.

Scope of the ICDE project

The ICDE project aims to include all possible 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 Pöyry, 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 requirements necessary for the development of 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, 2011).

Protection of proprietary rights

Procedures to protect 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 1.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 feed water 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, Rev. 1 "Common-Cause Failure Data Collection and Analysis System: Event Data Collection, Classification, and Coding:"

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.

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 probabilistic risk assessment (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;
- degraded ability of the component to perform its function;

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

- 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. 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 growing understanding of CCF events, the relative share of events that can only be modelled as "residual" CCF events is expected to decrease.

Annex 1.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 the 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 deficient 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/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 event is known, but does not fit in 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, 2011) 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 event cause and the coupling factor are broadly similar, with the combination of coding serving to give more detail as to the causal mechanisms. Selection is made from the following codes:

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 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, 2011) 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

The ICDE general coding guidelines (NEA, 2011) define corrective action as follows. 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.

Annex 1.D. CCF root cause analysis

By combining the coded information for the (apparent) event causes (EC), the corrective actions (CA) and the coupling factor (CF), insights regarding the root causes[6] of the CCF events can be gained. For each event, the event cause, corrective action and coupling factor are assigned to one of the three basic CCF root cause aspects listed below:

a) *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 the 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.

b) *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.

c) *Deficiencies in human actions (H):* This category comprises all events which happened because of erroneous human actions. Corrective actions for these events may involve training measures, further improvements of procedures and instructions or organisational improvements (e.g. more personal).

With the information originating from the EC, CA and CF, each event gets three basic root cause aspects. Due to the complex nature of the root causes for CCF events, the three aspects of an event are not always identical, so events may have one exclusive root cause (e.g. 3 x D), a predominant and a supporting cause (e.g. 2 x D and 1 x P) or no dominate cause (e.g. 1 x D, 1 x P and 1 x H).

In addition to the three basic root cause aspects listed above, the aspects “environmental” (E) and “unknown” (U) are used. “Environmental” is applied when some environmental factor (e.g. extreme weather, flooding) contributed to the event. The root cause focuses on the question of what was or must be done to prevent the event from reoccurring. It is almost never possible to adequately “change the environment”, so design or procedural improvements must be introduced to prevent reoccurrence of the event. Consequently, the aspect “environmental” could never be the predominant aspect. If “environmental” results in being the predominant root cause aspect, it is modified to be the supporting aspect and

6. As defined in IAEA-TECDOC-1756 the Root cause(s) is the most fundamental reason for an event or adverse condition, which if corrected will effectively prevent or minimise recurrence of the event or condition.

the resulting supporting aspect (D, P or H) is modified to be the predominant aspect. “Unknown” is applied in the rare case of incomplete or unknown coding.

The first root cause aspect is based on the coupling factor of the event. The resulting correlations are shown in Table 1.D.1.

Table 1.D.1. First root cause aspect – coupling factor

Coupling factor	**Root cause aspect**
Hardware	D
Hardware design	D
System design	D
Hardware quality deficiency	P
Operational	P
Maintenance/test schedule	P
M/T procedure	P
M/T staff	H
Operation procedure	P
Operation staff	H
Environmental (internal, external)	E
Environmental internal	E
Environmental external	E
Unknown	U

The second root cause aspect is based on the event cause of the event. To determine the root cause aspect, the coded information from the event cause and the corrective actions are used. If no clear assignment can be made with this information, the coupling factor is used in addition. The resulting correlations are shown in Table 1.D.2.

Table 1.D.2. Second root cause aspect – event cause

	Corrective action							
Event cause	**General administrative/procedure controls**	**Specific maintenance/operation practices**	**Test and maintenance policies**	**Design modifications**	**Diversity**	**Functional/spatial separation**	**Fixing of component**	**No Data (empty)**
Abnormal environmental stress	E	E	E	E	E	E	E	E
State of other component(s)	P	If CF "P" → P If CF "H" → H If CF "D" → D Else U	P	D	D	D	If CF "P" → P If CF "H" → H If CF "D" → D Else U	U
Design, manufacture or construction inadequacy	D	D	D	D	D	D	D	D
Internal to component, piece part	D	D	D	D	D	D	D	D
Maintenance	P	If CF "P" → P If CF "H" → H If CF "D" → D Else U	P	D	D	D	If CF "P" → P If CF "H" → H If CF "D" → D Else U	U
Human actions, plant staff	H	H	H	H	H	H	H	H
Procedure inadequacy	P	P	P	P	P	P	P	P
Unknown	U	U	U	U	U	U	U	U

The third root cause aspect is based in the corrective action which was implemented after the event. As well as for the event cause, the coupling factor is used if no clear assignment can be made. The resulting correlations are shown in Table 1.D.3.

Table 1.D.3. Third root cause aspect – corrective action

Corrective action	Root cause aspect
General administrative/procedure controls	P
Specific maintenance/operation practices	If CF "P" → P If CF "H" → H If CF "D" → D Else U
Test and maintenance policies	P
Design modifications	D
Diversity	D
Functional/spatial separation	D
Fixing of component	If CF "P" → P If CF "H" → H If CF "D" → D Else U
No Data (empty)	U

Annex 1.E. Workshop form

The workshop form included the following questions to answer:

1. Topical question: What type of inadequacy in the testing was observed? Choose one or more from the alternatives below or add one if no one is applicable.
    - **A. Extent of the test**
        1. Not all operating modes (power operation, during start-up, long term outage, etc.) covered by the test scope
        2. Not all operating conditions (e.g. emergency conditions) covered by the test scope
        3. Not all aspects on system level covered by the test scope
    - **B. QA of test/maintenance/modification**
        1. Inadequate process to ensure completeness of test
        2. Inadequate process to ensure adequacy of test
        3. Inadequate process to ensure validity of test
        4. Inadequate update of procedures after modification
    - **C. Performing the test**
        1. Inadequate instructions/checklists
        2. Inadequate use of equipment/instruments (e.g. not calibrated)
        3. Inadequate training of staff
        4. Omission of procedure step
    - **D. Verification of operability**
        1. Verification of operability after test
        2. Verification of operability after maintenance
        3. Verification of operability after modification
2. Describe the failure mechanism including cause of failure in a few words, for example *Vibration due to deficient installation led to cracks in fuel pipes*
3. Add the failure mechanism category and sub-category, and the failure cause category.
4. Specify the plant state (in operation, revision, etc.) when the event was detected

For question 5 or 6: 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 vendor, spare parts management, training of personnel, sufficient resources/staff, etc.)

5. If not complete CCF: Can you identify any **actual defences** that prevented all components to fail?
6. 6-1) If complete CCF: Can you identify any **possible defences** that could have prevented all components to fail?
   6-2) For other events: Can you identify any areas of improvement in order to prevent the event from happening again?

   If the event is of special interest to others, mark the event with applicable "Event Category(s)".