Nuclear Energy Agency

NEA/CSNI/R(2019)4

Unclassified English text only

17 March 2020

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Collection and Analysis of Common-Cause Failures due to Nuclear Power Plant Modifications

Topical Report of the Nuclear Energy Agency International Common-cause Failure Data Exchange Project

This document is only available in PDF format attached herein

JT03458837

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

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

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

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

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

Foreword

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

The purpose of the ICDE project is to allow multiple countries to collaborate and exchange CCF data so as to enhance the quality of risk analyses that include CCF modelling. Because CCF events are typically rare events, most countries do not experience enough of them to perform meaningful analyses. Input combined from several countries, however, yields sufficient data for more rigorous analyses.

The objectives of the ICDE project are to:

1) collect and analyse CCF events over the long term so as to better understand such events, their causes and their prevention;
2) generate qualitative insights into the root causes of CCF events, which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences;
3) 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;
4) generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries;
5) use the ICDE data to estimate CCF parameters.

The qualitative insights gained from the analysis of CCF events are made available in reports that are distributed without restrictions. It is not the aim of these reports to provide direct access to the CCF raw data recorded in the ICDE database. The confidentiality of the data is a prerequisite for operation of the project. The ICDE database is accessible only to members of the ICDE Working Group who have actually contributed data to the database.

Database requirements are specified by the members of the ICDE 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 members in the context of probabilistic safety assessment (PSA) / probabilistic risk assessment (PRA) reviews and application will use the data.

The ICDE project has produced the following reports, which can be accessed through the NEA website:

- Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(99)2], September 1999.
- Collection and analysis of common-cause failure of emergency diesel generators [NEA/CSNI/R(2000)20], May 2000.
- Collection and analysis of common-cause failure of motor operated valves [NEA/CSNI/R(2001)10], February 2001.
- Collection and analysis of common-cause failure of safety valves and relief valves [NEA/CSNI/R(2002)19], October 2002.
- Proceedings of ICDE workshop on the qualitative and quantitative use of ICDE Data [NEA/CSNI/R(2001)8], November 2002.
- Collection and analysis of common-cause failure of check valves [NEA/CSNI/R(2003)15], February 2003.
- Collection and analysis of common-cause failure of batteries [NEA/CSNI/R(2003)19], September 2003.
- Collection and analysis of common-cause failure of switching devices and circuit breakers [NEA/CSNI/R(2008)01], October 2007.
- Collection and analysis of common-cause failure of level measurement components [NEA/CSNI/R(2008)8], July 2008.
- Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(2013)2], June 2013.
- Collection and analysis of common-cause failure of control rod drive assemblies [NEA/CSNI/R(2013)4], June 2013.
- Collection and analysis of common-cause failure of heat exchangers [NEA/CSNI/R(2015)11], August 2015.
- ICDE workshop - collection and analysis of common-cause failures due to external factors [NEA/CSNI/R(2015)17], October 2015.
- ICDE workshop - collection and analysis of emergency diesel generator common-cause failures impacting entire exposed population [NEA/CSNI/R(2017)8], August 2017.
- Lessons learnt from common-cause failure of emergency diesel generators in nuclear power plants – a report from the international common-cause failure data exchange (ICDE) project [NEA/CSNI/R(2018)5], September 2018.
- ICDE 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], (forthcoming).
- ICDE topical report: collection and analysis of multi-unit common-cause failure events, [NEA/CSNI/R(2019)6], (forthcoming).

- Technical note on the ICDE project general coding guidelines, [NEA/CSNI/R(2019)12], (forthcoming).
- Summary of Phase VII of the International Common-Cause Data Exchange Project of Nuclear Power Plants Events, [NEA/CSNI/R(2019)3], June 2019.

Acknowledgements

The following individuals have significantly contributed to the preparation of this report through their own personal efforts: Gunnar Johanson (ÅF) and Mattias Håkansson (ÅF).

In addition, the International Common-cause Failure Data Exchange (ICDE) Working Group and the individuals with whom they liaise in all participating countries are recognised as important contributors to the success of this study. Olli Nevander, as the administrative NEA officer, has contributed to finalising the report.

Table of contents

Tables

Figures

Executive summary

The objective of the present report is to document a study that was performed on a set of common-cause failure (CCF) events. These events were derived from the International Common-cause Failure Data Exchange (ICDE) database, with the study focusing on events where failures occurred due to modifications in systems, components or procedures. The study is also based on a workshop held during an ICDE Steering Group meeting, where 53 ICDE events were assessed. The report is mainly intended for designers, operators and regulators to improve their understanding in relation to modifications-induced CCF risks and to provide insight into relevant failure mechanisms.

The report evaluates CCF events that occurred as a result of modifications, back-fitting, and/or replacements. However, there were no CCF events identified that were related to modifications resulting from a regulatory back-fit, i.e. relating to new or amended regulatory requirements or regulations.

The analyses in this report on plant modifications related to CCF events was undertaken according to the updated version of the general coding guidelines of the ICDE project, provided during phase seven. The updated version of general coding guidelines includes modified definitions for the terms: “event cause” and “CCF root cause”.

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

Based on the statistics of the collected events, a typical “failure due to modification”-event is an event with a hardware related failure cause, which is detected through a test during operation and corrected by design modifications or by general administrative/procedure controls.

For severe events (complete or partial CCF), instrumentation and control (I&C) modifications were most common. Several problems relate to modified protection devices of the main components (e.g. protection relays, contacts and wiring). This finding also underlines the importance of a complete and thorough system evaluation, including a full-featured test programme after modifications.

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

- Modifications to the safety systems of a nuclear power plant (NPP) have the potential to cause CCFs, especially CCFs that affect all redundant components at once.
- A stringent, comprehensive planning of the intended modifications should be performed, including assessment of possible interactions at the system-level.
- A comprehensive post-modification testing programme should be developed and implemented.
- Modifications of settings, testing procedures and maintenance procedures (e.g. change of lubrication, grease) should be comprehensively tested after the modification.

- If possible, modifications in redundant trains should not be implemented simultaneously so as to increase the chance that problems are identified through testing.
- Modifications to I&C systems and protection devices should be performed with special care, e.g. by using the method on time-separation. The method on time-separation of modifications means that a modification is carried out first only in one safety train during annual outage. With this procedure the modified safety train would go through annual functional tests and maintenance actions before similar modifications are made in all safety trains.
- CCFs due to the modification of sub-components are mostly related to the design of the sub-component itself and can be prevented by the owner via a thorough design evaluation and extensive review by the manufacturers.

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

List of abbreviations and acronyms

ANVS	Autoriteit Nucleaire Veiligheid en Stralingsbescherming / Authority for Nuclear Safety and Radiation Protection (Netherlands)
CCF	Common-cause failure
CNSC	Canadian Nuclear Safety Commission
CRDA	Control rod drive assembly
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee on the Safety of Nuclear Installations (NEA)
EDG	Emergency diesel generator
EE	Environmental external
EI	Environmental internal.
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat / Swiss Federal Nuclear Safety Inspectorate
ESD	Emergency shutdown system
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
ICDE	International Common-cause failure Data Exchange (NEA)
I&C	Instrumentation and control
IRSN	Institut de Radioprotection et de Sûreté Nucléaire / Institute for radiological protection and Nuclear Safety (France)
KAERI	Korea Atomic Energy Research Institute
MOV	Motor operated valve
NEA	Nuclear Energy Agency
NPSH	Net pressure suction head
NRA	Nuclear Regulation Authority (Japan)
NRC	Nuclear Regulatory Commission (USA)
OECD	Organisation for Economic Co-operation and Development
OP	Operation procedure
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
QA	Quality assurance
SRV	Safety relief valve
SSM	Swedish Radiation Safety Authority
STUK	Finnish Centre for Radiation and Nuclear Safety
TSO	Technical support organisation
UJV	Nuclear Research Institute (Czech Republic)

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

Corrective action: the corrective action describes the actions taken by the licensee to prevent the CCF event from reoccurring. The defence mechanism selection is based on an assessment of the event cause and/or coupling factor between the impairments.

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

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

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

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

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

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.

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

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

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

1. Introduction

In accordance with the objective of the International Common-cause Failure Data Exchange (ICDE) project to generate qualitative insights regarding the event causes of common-cause failure (CCF) events that can be used to derive approaches for their prevention, a workshop on CCF events with "failures due to modifications" was performed during the ICDE Steering Group meeting in May 2014. The objective was to study events where failures occurred due to modifications in systems, components or procedures. This report summarises the workshop results and presents CCF defence aspects concerning modifications from a CCF perspective.

The objectives of this report are:

- to describe the data profile of the ICDE events where failures occurred due to modifications;
- to develop qualitative insights of the reported events, expressed by event causes, coupling factors and corrective actions;
- to identify areas of improvement in the modification process, and possible or actual preventions for events from happening again;
- to give recommendations for CCF defences when considering modifications.

Chapter 2 presents a description of the event data "failures due to modifications". An overview of the contents of the database and summary statistics are presented in Chapter 3. Chapter 4 contains high-level engineering insights about CCF events. These insights are based on the modifications involved. Chapter 5 provides a summary and conclusions. References are found in Chapter 6.

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

2. Event data description

2.1. Preparation of event data "failures due to modifications"

The topic of the workshop was defined by the steering group. The group was interested in common-cause failure (CCF) events due to modifications. The selected CCF events were of wide variety but had one common denominator, i.e. modification. The types of modifications of interest were design modifications of components/systems, back-fitting of components with new or modified design, replacements of components with identical design and modification of settings. Events that occurred due to modified test procedures were included.

A modification or back-fit may result from a new or amended regulatory requirement. This process involves a detailed regulatory analysis to assess if new requirements are needed to ensure safe operation of NPPs. In this report, this is referred to as a "regulatory back-fit." The group did not identify any failure events that resulted from a regulatory back-fit. The modifications, back-fitting, and replacements discussed in this report are not related to new or amended regulations. These terms, as they are used in this report, are defined in Section 2.2.

In order to identify events which had failed due to modifications, several keywords were used to identify possible events, as seen in the figure below.[1]

The keywords resulted in 53 events after screening (out of about 1 700 ICDE events in the database). The screening aimed to exclude events where modifications were implemented as a corrective action but to include failures due to modification. If the event had been analysed in a previous ICDE workshop, the analysts' comments were included and used as additional information.

1. "FA-code D-mod" corresponds to failure cause category "design modification" in the failure analysis.

2.2. Modification, back-fitting and replacement

To identify and categorise a modification, the following terms are defined. The difference between modification, back-fitting and replacement is presented below.

Modification:	An adjustment made to an existing component, usually made to maintain or expand the functionality of the component. A modification may include a change to a component's shape, adding a feature or improving its performance. A modification is done by back-fitting or replacements, or can be related to modified maintenance/testing.
Back-fitting:[2]	Installation of updated (or additional) equipment to the existing component, to delay its obsolescence or to extend its functionality.
Replacement:	Substitution of a component without any functional changes. Yet the type/series or manufacturer of the component may change.

In this report, a modification can be back-fitting with new/modified design or a replacement (i.e. a one-to-one substitution). A modification can also be related to maintenance/testing, e.g. modified test procedure, modified settings or replaced lubricant.

2. A similar term to back-fitting is *retrofitting*: *modifying existing equipment or structures with additional or new components.*

3. Overview of database content

This Chapter presents an overview of the data set, which includes 53 events due to modifications. Tables are presented with the event parameters, i.e. event cause, coupling factor, corrective action, common-cause failure (CCF) root cause, detection method and event severity. The event parameters are defined in the International Common-cause Failure Data Exchange (ICDE) general coding guidelines [1], see Annex C.

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

- "Percent" is the percentage in relation to the subset of events which was analysed in the Workshop.
- "Relative occurrence" is the occurrence factor of the event parameter in relation to the complete ICDE database content.

3.1. Overview

The scope of the workshop and the distribution of the event severity[3] is presented in Table 3.1. Here it is seen that the events cover the whole event severity scale from complete CCF to incipient impairment. The most common event severities are "Complete impairment" (34%), "complete CCF" (23%) and "CCF impaired" (19%), where the first two correspond to different degree of failures of all components in the CCF group. Consequently, failures due to modifications are more likely to affect all components in the CCF group. In addition, the share of complete CCFs of the collected events (23%) is significantly larger than the share of complete CCFs in the complete ICDE database, which is about 9%. The share of centrifugal pumps and diesel generators events are higher compared to the complete ICDE database.

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)

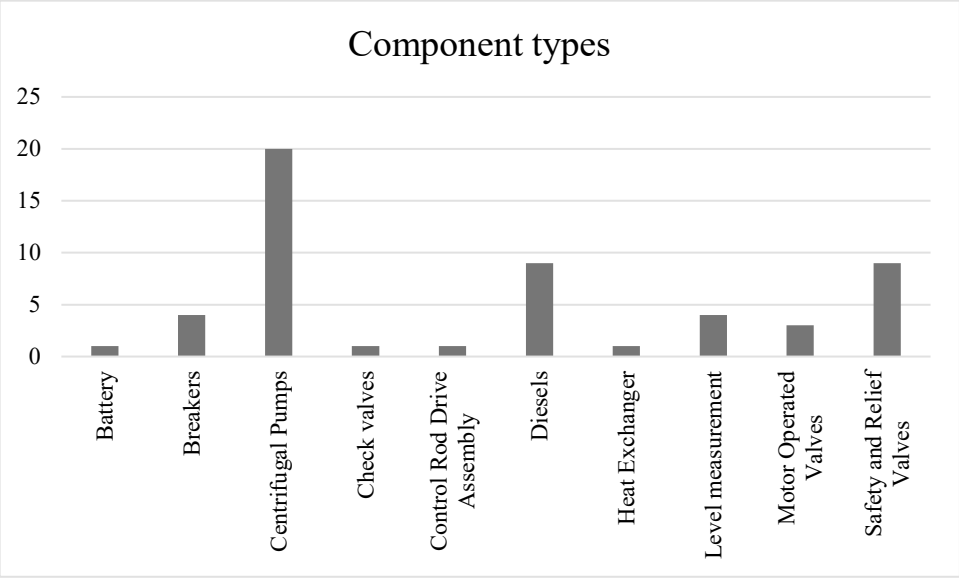
d) *Complete impairment* = All components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components. (all D or I in the impairment vector).

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

Table 3.1. The scope of the workshop. Distribution of components per event severity

	Event severity							
Component type	Complete CCF	Partial CCF	CCF Impaired	Complete Impairment	Incipient Impairment	Total	Percent	Relative occurrence
Battery				1		1	2%	40%
Breakers		2	1	1		4	8%	120%
Centrifugal pumps	8	1	5	3	3	20	38%	170%
Check valves	1					1	2%	30%
Control rod drive assembly	1					1	2%	20%
Diesels	1	2	2	4		9	17%	130%
Heat exchanger					1	1	2%	60%
Level measurement	1	1		2		4	8%	90%
Motor operated valves			1	1	1	3	6%	60%
Safety and relief valves			1	6	2	9	17%	110%
total	12	6	10	18	7	53	100%	
percent	23%	11%	19%	34%	13%	100%		
relative occurrence	250%	90%	70%	180%	50%			

Figure 3.1. Distribution of component types



3.2. Event causes

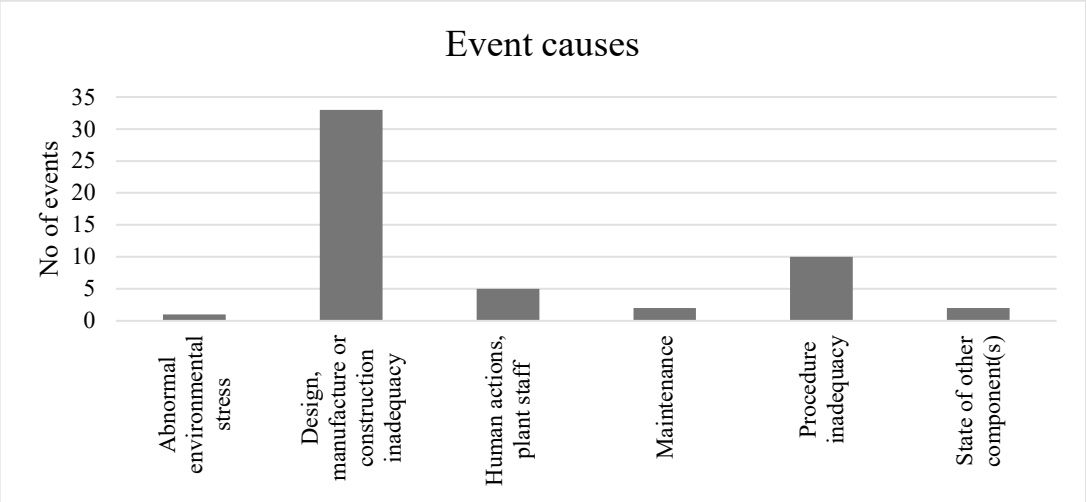
Table 3.2. and Figure 3.2. show the distribution of the events by event causes. The dominant event cause for the events was “design, manufacture or construction inadequacy” which accounted for 62% of the events. The relatively high occurring event causes can be correlation to the relatively high importance of these factors in the modification process. An example with this coding is an event where incomplete design of the system logic led

to start of both pumps without lube oil resulting in bearing damage of the pumps and complete CCF. This event showed deficiencies in planning/QA in the modification process.

Table 3.2. Distribution of event causes

	Event severity							
Event cause	Complete CCF	Partial CCF	CCF Impaired	Complete Impairment	Incipient Impairment	Total	Percent	Relative occurrence
Abnormal environmental stress				1		1	2%	40%
Design, manufacture or construction inadequacy	8	5	5	10	5	33	62%	200%
Human actions, plant staff	1	1		2	1	5	9%	100%
Maintenance	1		1			2	4%	80%
Procedure inadequacy	1		4	5		10	19%	150%
State of other component(s)	1				1	2	4%	50%
Total	12	6	10	18	7	53	100%	

Figure 3.2. Distribution of event causes



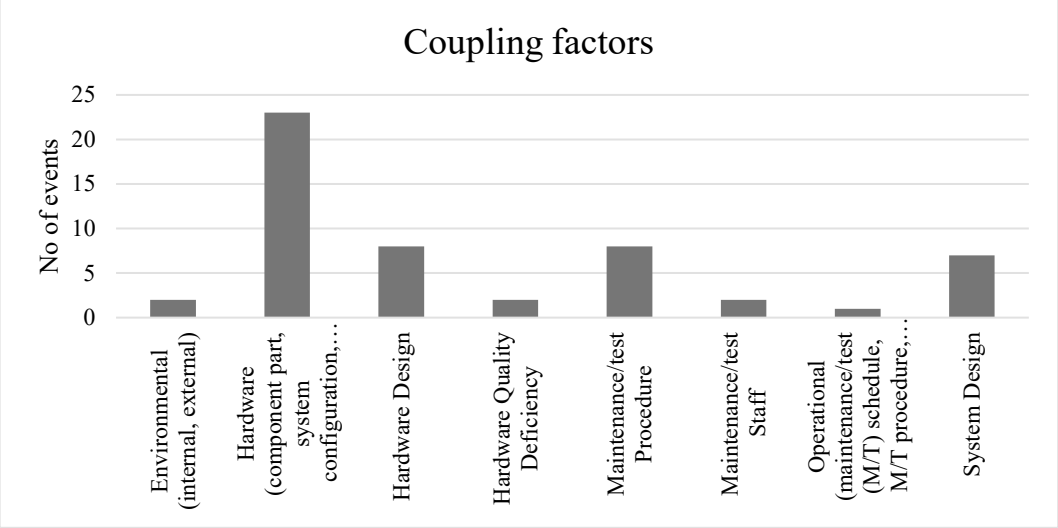
3.3. Coupling factors

Table 3.3. and Figure 3.3 show the distribution of the events by coupling factor. The dominant coupling factor group is hardware, which accounts for 75% of the events. One example of an event related to hardware is a complete CCF event where change of graphite gaskets caused both check valves to not reach the closed position during recurrent testing. This event underlined the lack of a requalification programme after the modification. The event was coded with the coupling factor "hardware design". Another event, coded with the coupling factor "environmental", is an event where a high temperature caused gumming-up of the lubricant, which caused the jamming of the three SRVs (one complete, one degraded and one incipient failure in the observed population). A new lubricant had only been introduced in the completely failed valve but was not tested under the right conditions.

Table 3.3. Distribution of coupling factors

	Event severity							
Coupling factor	Complete CCF	Partial CCF	CCF Impaired	Complete Impairment	Incipient Impairment	Total	Percent	Relative Occurrence
Environmental			1	1		2	4%	30%
Environmental (internal, external)			1	1		2	4%	170%
Hardware	9	6	8	12	5	40	75%	160%
Hardware (component part, system configuration, manufacturing quality, installation/configuration quality)	5	3	4	9	2	23	43%	230%
Hardware design	1	1	2	2	2	8	15%	90%
Hardware quality deficiency			1		1	2	4%	110%
System design	3	2	1	1		7	13%	180%
Operational	3		1	6	2	12	21%	60%
Operational (maintenance/test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)	1					1	2%	20%
Maintenance/test procedure	2		1	4	1	8	15%	110%
Maintenance/test staff				1	1	2	4%	80%
Total	12	6	10	18	7	53	100%	

Figure 3.3. Distribution of coupling factors



3.4. Corrective actions

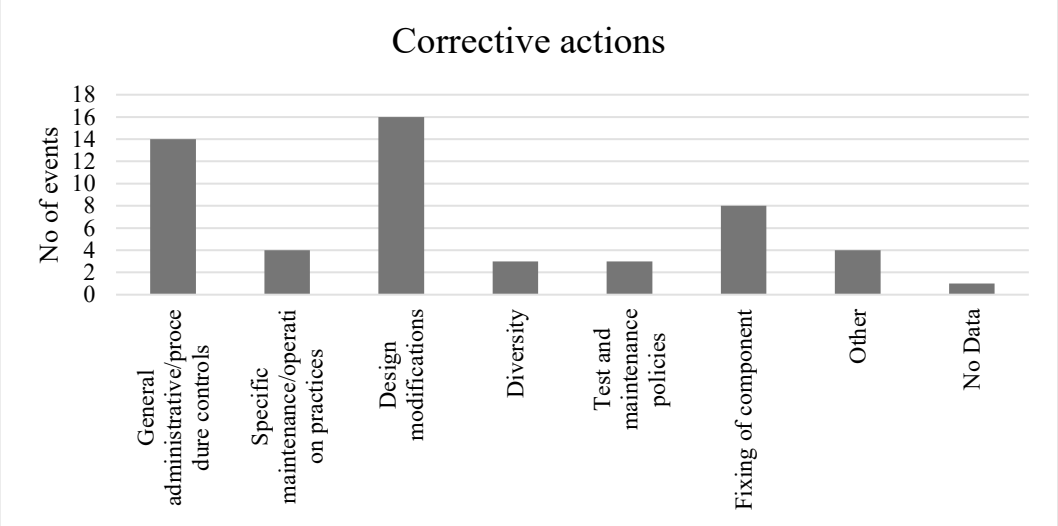
The distribution of the events for corrective actions is shown in Table 3.4. and Figure 3.4, where 30% of the corrective actions are made by “design modifications”, followed by “general administrative/procedure controls” and “fixing of component”. It is noteworthy that the most common corrective action was design modifications since the collected events are failures due to modifications. The statistics also shows the importance of revising the

procedures (test/maintenance) in the modification process. Relative to the entire database, enhancing diversity is an important corrective action for modifications.

Table 3.4. Distribution of corrective actions

	Event severity							
Corrective action	Complete CCF	Partial CCF	CCF Impaired	Complete Impairment	Incipient Impairment	Total	Percent	Relative Occurrence
General administrative/ procedure controls	4	2	3	4	1	14	26%	180%
Specific maintenance/ operation practices	1		1	2		4	8%	30%
Design modifications	4	1	4	3	4	16	30%	130%
Diversity	1			2		3	6%	220%
Test and maintenance policies	2			1		3	6%	50%
Fixing of component		2	2	2	2	8	15%	110%
Other		1		3		4	8%	160%
No Data				1		1	2%	130%
Total	12	6	10	18	7	53	100%	

Figure 3.4. Distribution of corrective actions



3.5. CCF root causes

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),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 elements provide one root cause aspect, which are combined into one CCF root cause. The possible CCF root cause aspects are:

4. See IAEA-TECDOC-1756 for more details

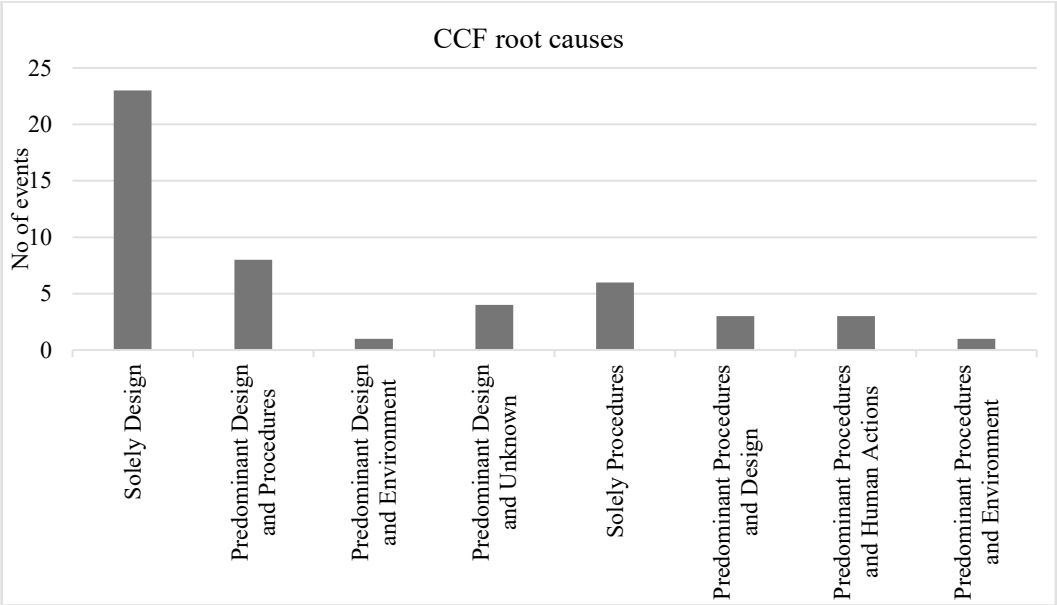
- Deficiencies in the design of components or systems (Design).
- Deficiencies in procedures (Procedures).
- Deficiencies in human actions (Human actions).

In addition to these three basic aspects, the supporting aspects “environmental” and “unknown” are used in case events due to external factors or events that are not completely coded. It is distinguished 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 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 event severity

	Event severity						
CCF root cause	Complete CCF	Partial CCF	CCF Impaired	Complete Impairment	Incipient Impairment	Total	Percent
Solely or predominant Design	8	5	7	12	4	36	68%
Solely design	6	3	4	6	4	23	43%
Predominant design and procedures	2	2	3	1		8	15%
Predominant design and environment				1		1	2%
Predominant design and unknown				4		4	8%
Solely or predominant procedures	4		2	5	2	13	25%
Solely procedures	2		1	3		6	11%
Predominant procedures and design	1		1		1	3	6%
Predominant procedures and human actions	1			1	1	3	6%
Predominant procedures and environment				1		1	2%
Solely or predominantly human actions				1	1	2	4%
Solely human actions				1	1	2	4%
No predominant CCF root cause		1	1			2	4%
Total	12	6	10	18	7	53	100%

Figure 3.5. Distribution of CCF root causes



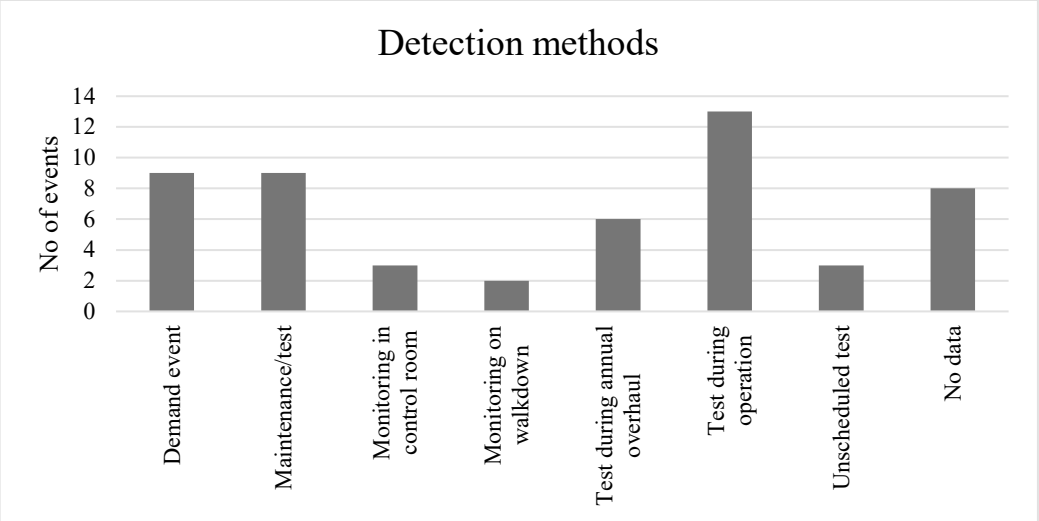
3.6. Detection method

Table 3.6.and Figure 3.6 contain the distribution of the events by detection method. The events were detected in several ways and the most common detection methods were “test during operation”, “demand event” and “maintenance/test”. The most severe events were either detected during test or a demand event.

Table 3.6. Distribution of detection methods.

	Event severity						
Detection method	Complete CCF	Partial CCF	CCF Impaired	Complete Impairment	Incipient Impairment	Total	Percent
Demand event	4		2	2	1	9	17%
Maintenance/test	1		1	6	1	9	17%
Monitoring in control room		1	1		1	3	6%
Monitoring on walkdown			1		1	2	4%
Test during annual overhaul	1	1	1	2	1	6	11%
Test during operation	5	2	4	1	1	13	25%
Unscheduled test				3		3	6%
No data	1	2		4	1	8	15%
Total	12	6	10	18	7	53	100%

Figure 3.6. Distribution of detection methods



4. Engineering aspects of the collected events

This Chapter includes the engineering aspects of the collected events. The analysis is based on questions listed in the workshop form in Annex E. The questions aim to be easy to understand and the workshop participants were also asked to mark interesting events according to the suggested codes, see Section 4.3. The workshop included 53 events to be analysed. The engineering aspects of the event analysis consisted of:

- What has happened?
  - involved modification;
  - time until failure after modification;
  - plant state when the event was detected;
  - failure mechanism descriptions.

- What can be done to prevent this from happening again?
  - areas of improvement in the modification process;
  - prevention – common-cause failure (CCF) defence aspects (possible defence if complete CCF and actual defence if not complete CCF).

- Interesting events

4.1. What has happened?

In order to analyse what happened at the 53 CCF events, it is shown which modifications were carried out, how much time passed before the failure occurred after modification, in which state the system was and which failure mechanism occurred. This will be categorised according to the possible answers from the workshop form and illustrated with tables and selected examples.

4.1.1. Involved modification

The distribution of involved modifications is presented in Table 4.1. The most common modification was "back-fitting with new/modified design" (62%) followed by "modifications related to maintenance/test" (32%). The category back-fitting is divided into the sub-categories *main component, sub-component, I&C and other.*

Table 4.1. Distribution of involved modifications

Involved modification	Total	
Back-fitting with new/modified design	33	62%
Main component	4	8%
Sub-component	18	34%
I&C	10	19%
Other	1	2%
Replacement with identical design	1	2%
Main component	1	2%
Modifications related to maintenance/test	17	32%
Other/unknown	2	4%
Total	53	100%

For the events categorised as "back-fitting with new/modified design", the most common modifications involved back-fitted sub-components followed by instrumentation and control (I&C).

Observed back-fitted main components, with new or modified design, involved new type of batteries, transmitters, back-fitting of over-pressure protection valves and new pilot valves of the pressuriser safety valves, one example for such event is:

- During revision outage inspection it was observed that five of eight pressuriser safety valves were not smooth-running as expected due to manufacturing defects of their bushings leading to corrosion. In the previous revision one year before the event, these valves replaced the former ones in the frame of a system modification.

Events with back-fitted sub-components involve six centrifugal pump events, six diesel generator events, three safety and relief valve events and one motor operated valve event, examples for such events are:

- The turbochargers of diesel generator units were replaced. Misjudgment of the new turbochargers wall inserts lead to an unanticipated resonance induced vibration resulting in fatigue failure of compressors impeller blade. Two of two diesels of unit one and one of unit two were unavailable.
- Triggered by an installation of reinforced sleeves on two trains' medium pressure safety injection systems their "over vibratory" alarms appeared performing a periodic test. Consequently, both redundancies were affected.

Events with back-fitted I&C involve two breaker events, five centrifugal pump events, two diesel generator events and a control rod drive assembly (CRDA) event. One example for such event is:

- At one instance, the emergency shutdown system (ESD) was modified to include an interlock to enable testing without triggering a reactor trip. An accumulation of errors during the design process meant that the final solution did not match the initial proposal and inadvertently disabled the ESD safety function.

Events with modifications related to maintenance/test involve two breaker and two centrifugal pump events with modified overcurrent-protection, three centrifugal pump events with modified testing procedures, one motor operated valve (MOV) and two safety relief valve (SRV) events and three level measurement events. One example for such event is:

- At one instance, a maladjustment of an overcurrent-protection relay had been introduced at the last revision one year ago, when the grading plan had been overhauled. During a test of the automatic change-over of the emergency power system one breaker switched on as designed, but opened one second later, of which two other breakers could have been effected. It was shown, that due to the switching behaviour of the breaker, the starting current could reach values above the set point of the overcurrent-protection. After the event the grading plan was revised again and the trigger-values of the overcurrent-protection for all breakers of this group had been changed.

4.1.2. Time until failure after modification

In Table 4.2, the time of operation of the components after the modification until failure or detection of faulty condition of component is shown. Here it can be seen that the time until failure differs significantly between the events. The time was not possible to specify for as many as 30% of the events. If excluding the unknown events, it can be concluded that most of the events occurred after a year or less after the modification.

Table 4.2. Distribution of time of operation until failure after modification

Time of operation	Total	
<1 month	7	13%
<1 year	13	25%
1 year	5	9%
>1 year	2	4%
>2 years	4	8%
>4 years	6	11%
Unknown	16	30%
Total	53	100%

As seen in Table 4.2., ten events were detected after more than two years of operation after the modification. Examples for such events are:

- An event with long latent time was an event where a modification design error removed a start permissive interlock contact of the centrifugal pumps. Under certain circumstances, this caused the auxiliary lube oil pumps to de-energised, and consequently the auxiliary feed water pumps tripped on low oil pressure. Further investigation showed that all motor driven auxiliary feed water pumps in unit one and two would be affected in the same way. A design error combined with insufficient post-modification testing led to this complete CCF event.
- The CRDA event presented in Section 4.1.1. The erroneous state after the modification persisted for more than two years.
- An example with short latent time (less than a month) was an event where a wiring error was discovered on a modification, which would prevent the diesel generators output breaker from closing. The error in wiring was the result of an incorrect drawing in the modification and resulted in a partial CCF. A contributing factor was the lack of testing after modification (did not functionally test the relay).

4.1.3. Plant state when the event was detected

The distribution of the plant state is presented in Table 4.3. The plant state was not possible to specify for 23% of the events. However, the information about the plant state is not considered essential in this engineering review.

Table 4.3. Distribution of plant state

Plant state	Total	
Full power	15	28%
Partial power	2	4%
Hot standby	3	6%
Shutdown (unit 1) + partial power (unit 2)	1	2%
Shutdown	13	25%
Outage	5	9%
Start up	2	4%
Unknown	12	23%
Total	53	100%

4.2. What can be done to prevent this from happening again?

To improve CCF defences against failures due to modifications, the engineering aspects of the collected events focus on identifying the involved modification and on preventions for events from happening again. The aim is to, e.g. to find what type of test procedures that could have detected the faulty modification, or what type of management aspects that should be considered when considering/implementing modifications in CCF groups.

4.2.1. Areas of improvement in the modification process

There were seven areas of improvements to choose from, see Table 4.3., where each event could be assigned to multiple areas (and thus not reflecting event counts). In Table 3.10., it is seen that the most common areas were “design of component” (28%), “testing procedure following modification” (25%) and “management system of plant” (24%).

Table 4.4. Distribution of identified improvement areas per involved modification

Involved modification	Areas of improvement in the modification process						
Back-fitting with new/modified design	a – Design of system or site	b – Design of component	c – Surveillance of component	d – Maintenance procedure for component	e – Testing procedure following modification	f – Operation procedure for component	g – Management system of plant[5]
Main component	2	1			1		
Sub-component	2	10		4	6	3	5
I&C	1	4			4		5
Other					1		1
Replacement with identical design main component							1
Other/unknown		2			2		
Modifications related to maintenance/test		5		7	6		7
Total marks	5	22	0	11	20	3	19

Modifications related to back-fitting

The 33 events categorised as modifications related to back-fitting with new or modified design were given a total of 50 marks, distributed over the improvement areas. Twelve events were severe (complete or partial CCF).

Analysis of different types of back-fitting shows that the improvement areas "design of component", "testing procedure" and "management system of plant" are the most important ones. For modifications with back-fitted main components, the improvement area "design of system" is assigned to two of the four events, which indicate a demand for complete system evaluation when changing main components. The improvement area "design of component" is assigned to 10 of the 18 events with back-fitted sub-components, which emphasises the importance of well-considered and planned design changes. For modifications with back-fitted I&C-components, the areas "design of component", "testing procedure" and "management system" are equally important.

Among the 12 severe events (complete or partial CCF), I&C modifications were most frequent. Several problems relate to modified protection to the main components (e.g. relays, contacts and wiring). Other problems relate to insufficient planning during the modification process, where improved management could have prevented the events from happening. The severe events are exemplified by the following observed events:

- Design error in the software of the digital protection relays led to a partial CCF of the centrifugal pumps (two of four pumps failed). The new relay type had been implemented during the last revision. As area of improvement, improved software testing and post-modification testing could potentially have detected the issue.
- Work in electrical cabinets led to inadvertent actuation of several breakers (partial CCF, three of six breakers with complete failure) when installing new overvoltage relays. The spurious operation occurred immediately. As improvement, better planning considering the risks associated in the work.

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

- Use of old damping values for the new transmitters led to activation of the automatic depressurisation. This was a partial CCF event where four of six transmitters had been modified and these transmitters were assessed as complete failures. The remaining two transmitters had not been modified yet. As improvement, the management should have checked the interfaces of the transmitters (compatibility with the old calibration values).

Modification – replacement

Only one event was interpreted as a one-to-one substitution. The event involved a replacement of a pump to the emergency feed water system. The new pump had different standards and flange piping which resulted in sealing leaks.

Modifications related to maintenance/test

The 17 events categorised as modifications related to maintenance/test were given 25 marks, distributed over the improvement area B (five marks), D (seven marks), E (six marks) and G (seven marks). Among the six severe events (complete or partial CCF), the main problem was related to insufficient net pressure of suction head (NPSH).

Events assigned to improvement area B "design of component" involve modification of settings for four out of five events, where the changes led to erroneous tripping of the overcurrent-protection breakers. Another observed problem relates to inadequate post-modification testing, where insufficient NPSH led to cavitation of the pumps during testing, due to error in the original design calculations.

Events assigned to improvement area D "maintenance procedure for component" involve mainly problems with modified settings (five/seven events), where improved maintenance procedure and independent work control could have prevented the events from occurring.

Events assigned to improvement area E "testing procedure following modification" involved modified testing procedures, which resulted in problems with insufficient NPSH. These events had high degree of severity (complete or partial CCF). Other problems related to modified settings involved inadequate post-modification testing.

Events assigned to improvement area G "management system of plant" involve two events where new grease caused problems. A better QA of manufacturer and spare part management were identified as possible improvements in the modification process. The remaining five events involved modification of settings. Failure to follow procedures/specification, inadequate training of personnel and insufficient work control were identified as possible improvements for these events.

4.2.2. Prevention – CCF defence aspects

A large span of CCF defence aspects need to be considered in the modification process to prevent against CCF. Examples of identified defence aspects to prevent events from happening again when implementing modifications are:

- Improved testing procedure could have discovered the failure, e.g. full load test after modification, relevant functional test.
- Improving maintenance procedure, training and briefings.
- Time-separated installation could have discovered the problem without degradation of both valves.
- Qualification of replacement spare part/grease.

- Better planning or QA of the modification.

As seen in Chapter three, most of the events have all their components affected and about 34% of the events are "complete impairments". For these events, actual observed aspects preventing the events to develop into a complete CCF are, for example:

- Failure detected before any damage to the pumps.
- Later re-analysis of the system discovered the situation.
- Vibration alarms revealed the problem before the pumps failed.
- The problem was discovered before the new transmitters were implemented on the third redundancy.

When implementing modifications/replacements all aspects from design to testing to QA of vendor need be taken into account. However, sometimes it can be very difficult to consider all aspects (e.g. unforeseen mechanism or difficult to detect) when implementing modifications, which is exemplified by the following observed event.

- New type of pistons rings with modified design were used (maintenance performed by valve supplier). The change of parts caused increased friction force and the piston required more moving force to re-close. As corrective action, the piston rings with modified design were replaced with the previously used design.

Five events were failures slowly developing over time and detected before developing into complete failures.

In summary, for many of the events it was concluded that improved testing procedures could have prevented the event from occurring. Other possible actions are also to have better work planning and better control routines after the modification. A review of the testing and maintenance procedures is very important when components are modified or replaced. In addition, time-separated implementation of modifications can reduce the possibility of all components to be affected by an erroneous modification.

4.3. Interesting events – discussion and examples

Marking of interesting events in the ICDE database consists of pointing out interesting and extra ordinary CCF event records with specific codes and descriptions, see ICDE general coding guidelines [1]. These records are important dependency events which are useful for the overall operating experience and can also be used as input to pre-defined processes for the stakeholders. An event can be applied to several codes. The ongoing devolvement of the codes has resulted in the codes "CCF new failure mechanism" and "CCF causes modification" to be excluded from further use by decision of the ICDE steering group. Consequently, these codes are not discussed in this report.

For many of the events it was possible to apply "interesting CCF event codes", see Table 4.5**.** Here it is seen that the most popular codes, except "no mark applicable", were "safety culture", "complete CCF" and "multi-unit CCF".

Table 4.5. 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.	12
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.	5
Component not-capable (3)	Event revealed that a set of components was not-capable to perform 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 safety function during the mission time.	6
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, Technical Support Organisation (TSO) and utility during construction and installation of a set of components.	2
CCF new failure mechanism (5)	Event revealed an unattended or not foreseen failure mechanism. The code gives information about a new CCF event revealed and a new failure mechanism, not earlier documented in the licensing documentation or operating history.	3
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 of how many common-cause component groups (CCCGs) were affected.	0
CCF causes modification (7)	Event causes major modification. The code gives information about a CCF event that has led to or will lead to a major plant or system or component modification.	8
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).	4
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

Interesting CCF event codes	Description Purpose	No. of events
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
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.	7
No code applicable (12)	Indicates that event has been analysed but the event is not considered to be highlighted and therefore none of the codes is applicable.	17
Other remarkable events (13)	Other remarkable event not covered by the other codes but worth to mark. The code gives information e.g. about an important new CCF failure mechanism, not earlier documented in the licensing documentation or operating history, or about a CCF event that has led to or will lead to a major plant or system modification.	0
Questionable coding (14)	Indicates that there are comments on the event coding in the analyst comment field.	0
Shutdown and decommissioning (15)	Events with special interest for plants in shutdown or decommissioning state. This code indicates events where CCF phenomena were observed which might be of special interest for non-power operation modes. It should not be used for components like the EDGs where the importance in all plant states is obvious.	0

An example with the code “complete CCF” is an event where maintenance work on main cooling water pumps led to loss of reactor coolant water pumps due to changed flow conditions in the common water intake for the pumps during the test. The maintenance procedure had been modified before the event occurred. As corrective action, the procedure was withdrawn and revised once again.

Another interesting event where unsuitable grease (not qualified for accident condition temperatures) was implemented by the manufacturer staff. They failed to follow the maintenance procedure/specification. This modification was part of back-fitting measures and applied to a fleet of plants. The use of unsuitable grease is difficult to reveal and was detected by an unplanned control. The event was assigned to the codes “component not-capable”, “safety culture” and “multi-unit CCF”.

5. Summary and conclusions

During the ICDE workshop on common-cause failure (CCF) events due to modifications, 53 events involving different component types from the International Common-cause Failure Data Exchange (ICDE) database were analysed with the aim of providing an overview of CCF mechanisms connected to modifications in systems, components, procedures and settings.

There were no common-cause failure (CCF) events identified that were related to modifications resulting from a regulatory back-fit, i.e. relating to new or amended regulatory requirements. The modifications, back-fitting and replacements discussed in this report are not related to compliance with new or amended regulations.

The collected events were analysed in Chapters 3 and 4 with respect to: degree of failure, type of involved modification, detection time after modification, failure cause, areas of improvement in the modification process and how to prevent the event from happening again. The report includes several CCF defence aspects and other interesting insights concerning modifications from a CCF perspective.

The assessment of the event severity showed that the share of events affecting all components of the operating procedure (OP), i.e. "complete CCF" (22%) or "complete impairment" (34%), is more than 50% of all analysed events. This underlines the importance of time-separated implementation of design modifications and of a covering post-modification testing programme.

The most common involved modification was "back-fitting with new/modified design" (62%) followed by "modifications related to maintenance/test" (32%). Events back-fitted with new/modified design involve modified sub-components followed by modifications of the I&C. The back-fitted sub-components involve modifications of main components, piece parts (e.g. piston rings and diaphragms, engine governors) and changes in ancillary systems (e.g. material change in system piping). The modified I&C events mainly involve added or modified protection logic or settings (e.g. overvoltage relays and control system cards). Modifications related to maintenance/test include modified test procedures, settings and modified overcurrent-protection set points.

When looking at the time of operation while the fault state of the affected components persisted undetected after the modification, it was unclear for many events how long the components had been in operation after the modification. This lack of information in the event description should be considered when forming conclusions. If only considering the large number of events, where the detection time is known, a clear majority of the events (about 70%) was detected within one year or less after the modification. Thereby, appropriate post-modification testing could have prevented some of the events from occurring. A few events were not discovered until over eight years after the modification. This indicates that neither the post-modification test programme nor the recurring testing could detect the faulty state of the components. Consequently, a review of the test procedures and test conditions should be included in the modification process.

When trying to identify possibilities to avoid CCFs after modifications, three main areas for improvement were suggested. These areas are "design of component" (28%), "testing procedure following modification" (25%) and "management system of plant" (24%).

For the severe events (complete or partial CCF), I&C modifications were most common. Several problems relate to modified protection devices of the main components (e.g. protection relays, contacts and wiring). This finding also underlines the importance of a full-featured test programme after modifications. The significant share of CCF events in the category "management system of plant" indicates that the whole planning process (including the planning of the tests afterwards) is highly important while implementing modifications for safety relevant systems.

For back-fitted main components, a complete and thorough system evaluation is important. Examples for such events, which result from the interaction between the modified component and the rest of the system, are several severe events, which were related to an insufficient net pressure of suction head NPSH. For back-fitted sub-components, it has been shown that problems related to the design of the sub-component itself are the most prominent reason for CCF while implementing such modifications.

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

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

For some events, these defences prevented the failure all components. For other events, the failures were slowly developing over time and detected before developing into complete failures.

Regarding the ongoing development of the ICDE database, it was also established that describing the failure mechanism was a good start in the analysis process. The failure mechanism describes the observed event and influences leading to a given failure. The description usually identifies reasons for why the event happened, which is necessary for identifying actions that can prevent the event from reoccurring. This leads to suggested areas of improvements in the modification process.

Noting interesting events identifies important CCF events, which is useful for overall operating experience. About two thirds of the events were marked with at least one

interesting code. The most common codes were “safety culture”, “complete CCF” and “multi-unit CCF”.

6. References

1. NEA (2011), *International Common-Cause Failure Data Exchange ICDE General Coding Guidelines – Updated Version*, NEA/CSNI/R(2011)12, OECD, Paris.

2. IAEA (2014), *Root Cause Analysis Following an Event at a Nuclear Installation: Reference Manual,* IAEA-TECDOC-1756, IAEA, Vienna.

Annex A. – Overview of the ICDE project

Appendix A contains information regarding the ICDE project.

Background

Common-cause failure (CCF) events can significantly impact the availability of safety systems of NPPs. 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 various countries. A further impediment is that descriptions of reported events and their root causes and coupling factors, which are important to the assessment of the events, are usually written in the native language of the countries where the events were observed.

To overcome these obstacles, the preparation for the International Common-cause Failure Data Exchange (ICDE) project was initiated in August of 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 current eight term began in 2019 and will end in 2022. Member countries under the current Agreement of OECD/NEA and the organisations representing them in the project are: Canada (CNSC), Czech Republic (UJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), Korea (KAERI), Netherlands (ANVS), Spain (CSN), Sweden (SSM), Switzerland (ENSI), and United States (NRC).

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

Scope of the ICDE project

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

Data collection status

Data are collected in an MS.NET based database implemented and maintained at ÅF, Sweden, the appointed ICDE operating agent. The database is regularly updated. It is operated by the operating agent following the decisions of the ICDE steering group.

ICDE coding format and coding guidelines

Data collection guidelines have been developed during the project and are continually revised. They describe the methods and documentation 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 [1].

Protection of proprietary rights

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

Annex B. – Definition of common-cause events

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

- Unavailability of a specific set of components of the system, due to a common dependency, for example on a support function. If such dependencies are known, they can be explicitly modelled in a probabilistic safety assessment (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" common-cause failures (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, Revision one "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 International Common-cause Failure Data Exchange (ICDE) project, focus will be on CCF events with total as well as partial component failures that exist over a relevant time interval[6]. 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;
- 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

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

of its components is “complete failure to perform its function” and where these fault states exist simultaneously and are the direct result of a shared cause. Thus, in the ICDE project, we are interested in collecting complete CCF events as well as partial CCF events. The ICDE data analysts may add interesting events that fall outside the ICDE event definition but are examples of recurrent - eventually nonrandom - 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 C. – ICDE general coding guidelines

Event cause

In the International Common-cause Failure Data Exchange (ICDE) database the Event cause (EC) describes the direct reason for the component's failure. For this project, the appropriate code is the one representing the common-cause, or if all levels of causes are common-cause, the most readily identifiable cause. The following coding was suggested:

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

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

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

H Human actions. This represents causes related to errors of omission or commission on the part of plant staff or contractor staff. This category includes accidental actions, and failure to follow procedures for construction, modification, operation, maintenance, calibration, and testing. This category also includes 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 [1] define coupling factor (CF) as follows. The CF 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 CF 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' CF.

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" CF.

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 CF.

Detection method

The ICDE general coding guidelines [1] 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 [1] define corrective action (CA) as follows. The CAs field describes the actions taken by the licensee to prevent the CCF event from reoccurring. The defence mechanism selection is based on an assessment of the event cause and/or CF 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 program modification. The modification includes item such as staggered testing and maintenance/ operation staff diversity.

G Fixing component

O Other. The CA is not included in the classification scheme.

Annex 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 CCF root causes[7] of the common-cause failure (CCF) events can be gained. For each event, the event cause, the corrective action and the 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 correct and under circumstances (ambient temperature, fluid temperature, pressure etc.) within the expected limits. In general, these events require changes to hardware as CA.

b) *Procedural or organisational deficiencies (P)*: This category comprises all events where a) wrong or incomplete procedures or where applied and followed and b) events which happed 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 CA.

c) *Deficiencies in human actions (H)*: This category comprises all events which happened because of erroneous human actions. CAs 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 event causes (EC), the corrective actions (CA) and the coupling factor (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. 3xD), a predominant and a supporting cause (e.g. 2xD and 1xP) or no dominate cause at all (e.g. 1xD, 1xP and 1xH).

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, etc.) has contributed to the event. The root cause focuses on the question what was or must be done to prevent the event from reoccurrence. 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 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 CF of the event. The resulting correlations are shown in Table A D.1.

7. 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*.

Table A D.1. First root cause aspect – Coupling factor (CF)

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 CAs are used. If no clear assignment can be made with this information, the CF is used in addition. The resulting correlations are shown in Table A D.2.

Table A 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 CA which was implemented after the event. As well as for the event cause, the CF is used if no clear assignment can be made. The resulting correlations are shown in Table A D.3.

Table A 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 E. – Workshop form

The workshop form included the following questions to answer:

1. Describe the type of modification involved.
2. How long was the component in operation after the modification?
3. Specify the plant state (in operation, revision, etc.) when the event was detected.
4. Can any areas in the modification process be identified in order to prevent the event from happening again? If so, assign them to the following categories:
   a. Design of system or site.
   b. Design of component.
   c. Surveillance of component.
   d. Maintenance procedure for component.
   e. Testing procedure following modification.
   f. Operation procedure for component.
   g. Management system of plant (QA of vendor, spare parts management, training of personnel, sufficient resources/staff etc.).
5. Describe the failure mechanism[8] including cause of failure in a few words, for example, *Vibration due to deficient installation led to cracks in fuel pipes.*
6. What has or could have prevented all components to fail (if so)? Example: *Failure was slowly developing over time and was detected before all components failed.*
7. Mark the event with any of the interesting event codes.

8. The history describing the event and influences leading to a given failure.