Nuclear Safety
NEA/CSNI/R(2019)6
November 2022
www.oecd-nea.org

ICDE Topical Report

Collection and Analysis of Multi-Unit Common-Cause Failure Events

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CSNI/R(2019)6

Unclassified English text only

2 November 2022

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

ICDE Topical Report

Collection and Analysis of Multi-Unit Common-Cause Failure Events

This document is available in PDF format only.

JT03506441

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 (CSNI)

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, the International Common-cause Failure Data Exchange (ICDE) Project was initiated by several Nuclear Energy Agency (NEA) member countries in 1994. In 1997, the NEA Committee on the Safety of Nuclear Installations (CSNI) formally approved this project to be carried out within the NEA framework. Since then, the project has operated over six consecutive terms (the last term being 2015-2018).

The purpose of the ICDE project is to allow countries to collaborate and exchange common-cause failure (CCF) data to enhance the quality of risk analyses, which 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, are 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 so as to better understand such events, their causes, and their prevention;
- generate qualitative insights into the root causes of CCF events that can help establish approaches or mechanisms to prevent CCF events or mitigate their consequences;
- establish a mechanism for efficient feedback of experience gained in connection with CCF phenomena, including the development of defences against their occurrence, such as indicators for risk-based inspections;
- generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries; 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 database.

Database requirements are specified by the members of the ICDE project working group and are fixed in guidelines. Each member with access to the ICDE database is free to use the collected data. It is assumed that the data will be used by the members in the context of PSA/PRA reviews and application.

The ICDE project has produced the following reports, which can be accessed through the NEA website (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 Populations [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] (forthcoming).
- ICDE Topical report: Collection and Analysis of Multi-Unit Common-Cause Failure Events, [NEA/CSNI/R(2019)6] (this report).

Acknowledgements

The following individuals have contributed significantly to the preparation of this report by their personal effort: Mr Gunnar Johanson (ÅF Pöyry), Mr Mattias Håkansson (ÅF Pöyry), Mr Dong-San Kim (KAERI).

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. Dr Diego Escrig Forano was the administrative NEA officer 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 International Common-cause Failure Data Exchange (ICDE) Project. The topic was *multi-unit CCF events.*

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

The analyses in this report on multi-unit CCF events were carried out according to the updated version of the general coding guidelines of the ICDE provided during phase seven. The updated version of general coding guidelines includes modified definitions to the terms "event cause" and "CCF root cause".

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

- Multi-unit events were observed for a wide range of component types. Emergency diesel generators and centrifugal pumps accounted for more than 50% of the events.
- The most common CCF root cause (nearly 60%) for multi-unit CCF events was deficiency in the design of components and systems. Design is therefore significantly overrepresented compared to the total observed CCF event population.
- Events with observed environmental deficiencies were caused by harsh environmental conditions, such as severe weather or abnormal debris in a raw water source, that usually require design improvements to prevent reoccurrence.
- About 10% of the events were complete multi-unit CCF events.

It should be recognised that 57 events were caused by internal factors, where 27 of these events were related to "identical design" (for example, same design of components/systems, operating environment or installation) and 17 to "organisational aspects" (mainly by test and maintenance procedures). In total, 14 events were caused by external factors, with 10 of these events related to "shared structures, systems and components (SSCs)" (for example, units with shared water intake channel). Four of the nine complete CCFs were caused by shared SSCs.

The engineering aspects of the internal and external multi-unit CCF events yielded the following lessons learnt for design and operation:

- Feasible defence strategies against internal multi-unit CCF events are well-functioning testing procedures, maintenance procedures, operating experience feedback, skilled personnel, etc. Adequate and robust system/component design is the fundamental defence against complete CCFs. Also, some failures develop slowly over time and can be detected before turning into complete CCFs.
- Feasible defence strategies against external multi-unit CCF events are improving the "design of system or site", such as the design of water intake; adding back-flushing capability, cleaning of strainers, etc. Also, improved surveillance/maintenance is a feasible defence to detect the problems before the components fail.

The multi-unit CCF events identified in this report can provide useful insights to inform multi-unit probabilistic safety assessment (MUPSA) modelling. The external factor events can provide insights relevant to the modelling of physical connections and dependencies across unit boundaries. The internal factor events can provide insights relevant to defining new CCF groups by combining common-cause component groups across units at the site.

The two reports "Provision against Common-Cause Failures by Improving Testing" [NEA/CSNI/R(2019)5] (forthcoming) and "Collection and Analysis of Multi-Unit Common-Cause Failure Events" [NEA/CSNI/R(2019)6] (this report) 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

AFWS	Auxiliary feed-water system
ANVS	Autoriteit Nucleaire Veiligheid en Stralingsbescherming (Netherlands)
CCF	Common-cause failure
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee on the Safety of Nuclear Installations
CV	Check valves
EC	Event causes
EDG	Emergency diesel generator
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat (Switzerland)
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
HE	Heat exchanger
HVAC	Heating, ventilation, and air conditioning
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)
LOCA	Loss-of-coolant accident
LOOP	Loss of off-site power
MOV	Motor operated valves
MUPSA	Multi-unit site PSA
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission (United States)
NRA	Nuclear Regulatory Authority (Japan)
OECD	Organisation for Economic Co-operation and Development
QA	Quality assurance
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
PWR	Pressurised water reactor

RWST	Raw water storage tank
SBO	Station black-out
SRV	Safety and relief valves
SSC	Structures, systems and components
SSM	Swedish Radiation Safety Authority (Sweden)
STUK	Radiation and Nuclear Safety Authority (Finland)
TSO	Technical support organisation
UJV	Nuclear Research Institute (Czech Republic)

NB: Annex 1.C lists the acronyms from the ICDE General Coding Guideline (NEA, 2011).

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

Shared cause factor: allows the analyst to express their 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

This report was drafted in accordance with the objective of the ICDE project to generate qualitative insights into the causes of CCF events that can be used to improve prevention. The ICDE steering group organised two workshops on the topic of multi-unit events, in April 2015 and October 2016. The main objective was to study events that occurred at multiple units at the same site, so-called multi-unit events. This report summarises the workshop results and presents CCF defence aspects concerning multi-unit events from a CCF perspective.

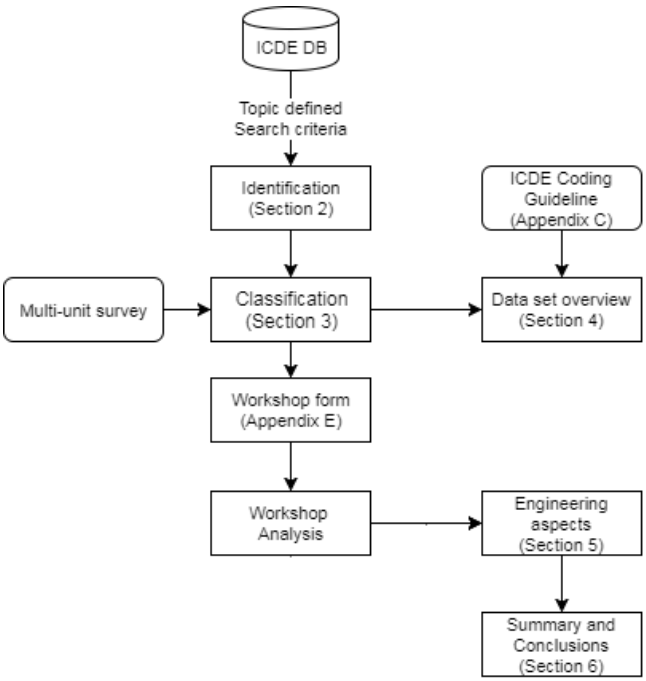
The objectives of this report are:

- to describe the data profile of the ICDE events that occurred at multiple units at the same site;
- to develop qualitative insights of the multi-unit events, expressed by event causes, coupling factors, and corrective actions;
- to identify correlation factors, internal and external factors, that led to the event that affected multiple units;
- to identify areas of improvement and possible/actual preventions against such events happening again; and
- to give recommendations for CCF defences related to multi-unit issues.

Sections 2 and 3 present the multi-unit event identification and classification process. Section 4 presents an overview of the included multi-unit events with their CCF event parameters. Section 5 contains the engineering insights about the multi-unit CCF events, supported by the failure mechanism descriptions. These insights are based on the identified correlation factors. Section 6 provides a summary and conclusions. References are found in the dedicated section at the end of the report. Figure 1.1 below presents the report structure and analysis process.

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 present the definition of common-cause failures, 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.

Figure 1.1. Report structure and analysis process



2. Identification of multi-unit events

As part of the ICDE failure analysis process, the project developed criteria for marking interesting CCF events. These events involve interesting, unique or subtle dependencies, and they often provide useful lessons for developing defences against CCFs. One of the interesting event codes used in the ICDE failure analysis is for a CCF event affecting multiple reactor units. The search for multi-unit event candidates was primarily based on this interesting event category (i.e. the event is marked as multi-unit event in previous workshops). The database was also searched using different keywords to identify additional multi-unit events, such as *multi, fleet, unit 1 and 2*.

The search for events to be marked as "multi-unit" also included other possible keywords. These can include a second plant's name, which countries often use in the event description. Also, countries contributed events that were not covered/identified by the above search criteria.

The CCF events submitted to the ICDE are typically reported for single reactor units. If an event occurs in several plants, separate ICDE events are normally provided. Therefore, a multi-unit event can be reported as multiple ICDE events.

A multi-unit event consists of individual ICDE events of the same type that share a multi-unit dependency. These dependencies are defined in Section 3.

The analysis covers 87 multi-unit events, which include 192 ICDE events. The reason for the difference in numbers is that ICDE events are in most cases counted by component groups (only one component group affected per event) while multi-unit events usually affect component groups in more than one unit, so in general each multi-unit event comprises two or more ICDE events. Table 2.1 presents the distribution of ICDE events and multi-unit events per component type.

Table 2.1. ICDE events and multi-unit events

	ICDE events		**Multi-unit events**	
Component type	**Count**	**Percentage**	**Count**	**Percentage**
Battery	25	13%	9	10%
Breakers	3	2%	2	2%
Centrifugal pumps	56	29%	22	25%
Check valves	10	5%	5	6%
Control rod drive assembly	1	1%	1	1%
Diesels	51	27%	26	30%
Heat exchanger	2	1%	2	2%
Level measurement	10	5%	4	5%
Motor operated valves	7	4%	6	7%
Safety and relief valves	27	14%	10	11%
Total	**192**	**100%**	**87**	**100%**

3. Classification of multi-unit events

3.1 Basis for classification

This chapter defines the event classification that was developed to assess multi-unit events. The 87 multi-unit events were classified with respect to: degree of multi-unit correlation expressed by internal and external correlation factors; simultaneity between the events; degree of severity; and whether the events occurred at different plant sites. Two primary categories of multi-unit event correlation factors are defined: internal factors and external factors. The internal factors involve failures relating to the design of systems and components, maintenance procedure or other organisational factors that are common between multiple units. The external factors involve a physical connection, an external connection or a shared external environment between the affected systems and components. A third category of multi-unit events is defined to account for fleet CCF events. These events involve the same or similar types of CCF events that occur at different sites. Additionally, a multi-unit site survey was conducted by the ICDE steering group members. This survey collected information on all multi-unit sites in the participating member countries. The survey provided useful information for understanding the CCF dependencies that are observed in the multi-unit events.

3.1.1 Internal factors – shared cause – dependent multiple CCF events at a site

These CCF events involve two or more reactor units located at the same site. The same CCF failure mechanism is present on multiple units at the site within a time frame that results in a not negligible chance of a simultaneous failure. The shared cause of the observed multi-unit CCF event was not a direct physical connection (e.g. common water intake, common electricity supply) but the design of systems and components, maintenance procedure or other organisational factors that are common between the multiple units. Examples of shared causes include:

- design, construction, manufacturing deficiencies;
- deficient maintenance/test procedures;
- insufficient safety culture management.

For the purpose of a multi-unit site probabilistic safety assessment (MUPSA), new CCF groups may need to be defined to combine common-cause component groups across all units at the site. For example, a two-unit site may need to double the common-cause component group (CCCG) size to include all components at the site.

3.1.2 External factors – shared environment or physical connection – dependent multiple CCF events at a site

These CCF events involve two or more reactor units located at the same site. There exists a physical connection, an external connection or a shared external environment between

the affected systems and components. The same type of CCF event is present at multiple units at the site in a short timeframe within the same test interval.[1] Examples include:

- external connection on e.g. service water system, electrical grid connection;
- clogging of heat exchangers at multiple units due to condition of common water source;
- equipment for multiple units is in the same room or location and susceptible to the same environmental conditions, e.g. high temperature, humidity.

For the purpose of a multi-unit site PSA, the physical connections and dependencies of cross-unit boundaries may need to be explicitly modelled in the PSA. In some cases, new CCF groups may need to be defined for not-yet-modelled dependencies across all units at the site.

3.1.3 Fleet CCF events – multiple CCF events occurring at multiple sites

These events involve the same or similar types of CCF events occurring at different sites. There exists, however, no physical connection between the affected systems and components and other sites. The same type of CCF events is present on all affected units. The time interval for the occurrence of these events at different sites can exceed the test intervals that are typically used in defining single unit CCF events. These events highlight the importance of having an effective programme for sharing and addressing operating experience among plants/sites with similar systems and components. Examples of observed fleet events include:

- Use of improper pump motor connectors at several pumps. In case of loss-of-coolant accident (LOCA) or steam pipe rupture, the generated steam would have created a short circuit in the connectors that might lead to a failure of the pumps.
- Use of unsuitable grease at several pumps after the manufacturer stopped the production of the formerly used grease.

For the purpose of a multi-unit site PSA, there is typically no direct dependency between similar CCF events occurring at different sites. Therefore, these events would not be modelled in a MUPSA. However, identifying these events can provide insight to the types of important CCF events to include in a MUPSA.

3.1.4 Multi-unit survey

To investigate the need for a MUPSA, a survey on multi-unit aspects was conducted within the ICDE steering group. Six countries participated in the survey, covering 74 sites and 205 reactor units. A few shared aspects were selected to be relevant for a MUPSA model. The shared aspects were design, shared systems, mobile equipment at site, grid setup, heat sink, site layout, management, organisation and staff. Depending on whether the units were located at a "site", a single site could have multiple entries in case not all units at a site share the same multi-unit aspects and therefore so-called "sub-sites" were formed. Table 3.1 presents the findings from the survey, which includes important aspects to consider for a MUPSA model.

1. The timeframe could be longer if the latent time is longer than the test interval.

Table 3.1. Findings from the multi-unit survey

Shared aspect	Findings
Design	A short description of reactor type and the site set-up were given, e.g. PWR twin-units. It was also indicated if the site consisted of sub-sites.
Shared systems	The survey results show that multiple types of systems can be shared between the units. The main categories of shared systems are: • **pumps systems** (both auxiliary systems and emergency feed-water systems); • **electrical systems** (such as swing diesel, gas turbines, transformers and buses); • **tanks** (such as RWST, condensate storage tanks); • **structures** (such as auxiliary-, intake- and turbine building); • **other** (such as control room, instrument air system, HVAC).
Mobile equipment	The types of shared mobile equipment at a site can be diesels, pumps and gas turbines.
Grid	The grid connection is either common or separate. Most sites have a common switchyard.
Heat sink	The types of shared heat sinks are common intake channel, common water source (sea, ocean, river, lake, pond, bay, and reservoir), cooling tower (mechanical or natural) and water discharge tunnel.
Location and distance apart	The distances between reactor buildings vary between 50 and 300 metres while sub-sites are separated by 300-1 000 metres.
Management	Most of the sites share a common owner and none of sub-sites had different owners. Thereby, the management aspect for a MUPSA model should be considered when the site has a common owner since it is more susceptible to multi-unit CCF events.
Organisation	It was asked whether the maintenance, test and operation procedures are shared at the site. The results show that these can be shared, or partly shared and in some cases not shared at all. Thus, this is an important aspect to consider in a MUPSA model.
Staff	Some sites share maintenance and test personnel at the site and some do not share personnel. No site had shared operation staff.

3.2 Concluded multi-unit event classification factors

3.2.1 Overview

The aspects from the multi-unit survey (Section 3.1.4) and the definitions in Sections 3.1.2 and 3.1.3 can be connected to the correlation factors used in the workshop form, see Table 1.E.1 in Annex 1.E. By combining these, final multi-unit classification factors can be defined, as in Figure 3.1. These factors are further discussed in Section 5.

Figure 3.1. Multi-unit classification, internal and external factors

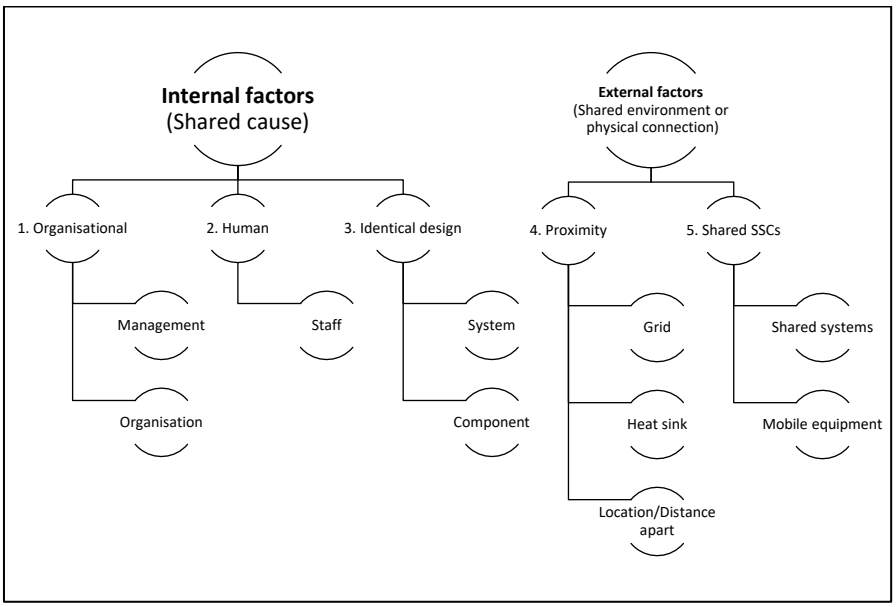


Table 3.2 presents the resulting classification of the multi-unit events per component type.

Table 3.2. Multi-unit event classification per component type

Component type	Multi-unit event category			Total	Percentage
	1. Internal factors (Shared cause)	2. External factors (Shared environment or physical connection)	3. Fleet CCF events		
Battery	7		2	9	10%
Breakers		1	1	2	2%
Centrifugal pumps	16	4	2	22	25%
Check valves	4		1	5	6%
Control rod drive assembly		1		1	1%
Diesels	16	7	3	26	30%
Heat exchanger	2			2	2%
Level measurement	1		3	4	5%
Motor operated valves	4	1	1	6	7%
Safety and relief valves	7		3	10	11%
Total	**57**	**14**	**16**	**87**	**100%**

3.2.2 Simultaneity between events

The simultaneity between the individual ICDE events within a multi-unit event is important to determining whether the classify the events as occurring within a short time interval or recurring. The classification identifies:

- If the events are multi-unit events (occurred within one year) or recurring events (more than one year in between the events).

- If the events affected multiple units at one site or multiple units at several sites:
  - ***Site event:*** The events have affected multiple units at one site.
  - ***Fleet event:*** The events have affected multiple units at several sites.

Table 3.3 presents the classification of the multi-unit events. Here it is seen that most of the events are site events and occurred within one year. The criteria of "within one year" was selected to include events with long latent time. Among these, many events occurred on the same day or within a month of each other, i.e. the simultaneity between the individual events was high. The fleet events are discussed in Section 3.2.3.

Table 3.3. Classification of simultaneity of multi-unit events

Simultaneity of multi-unit events	Number of multi-unit events	Percentage
Site events	**71**	82%
Within one year	67	77%
Within one year and recurring (more than one year)	1	1%
One event reported, other event dates unknown	2	2%
More than one year	1	1%
Fleet events	**16**	18%
Total	**87**	**100%**

3.2.3 Fleet events

A total of 16 fleet events[2] were identified and about two-thirds of the events occurred within one year, see Table 3.4. The number of sites affected ranges from two to five different sites. For some events, it was not clear how many sites were affected. All the identified fleet CCF events were correlated by internal factors.

Table 3.4. Fleet CCF events

Fleet events	Number of fleet events	Percentage
Fleet event (two different sites)	5	31%
Fleet event (three different sites)	2	13%
Fleet event (four different sites)	5	31%
Fleet event (five different sites)	1	6%
Fleet event (unknown number of sites)	3	19%
Total	**16**	**100%**

3.2.4 Severity – impairment vectors

The multi-unit event severity is a combination of the ICDE events component impairment vectors. For example, if there are two events with vectors "CC" and "DD", the resulting

2. Fleet events were screened out in the second data analysis workshop (there was no dedicated search for additional fleet events). Thus, the number of fleet events in the database may be greater than those included in this report.

vector is “CCDD” and the multi-unit event severity is therefore “Partial CCF”. The multi-unit event severity categories are defined as:

a) *Complete CCF* = All components are completely failed (i.e. all elements in impairment vector are C).

b) *Partial CCF* = At least two components completely failed (i.e. at least two C in the impairment vector, but not complete CCF).

c) *CCF Impaired* = At least one component 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 are affected, no complete failures but complete impairment. Only incipient degraded or degraded components (i.e. all D or I in the impairment vector).

e) *Incipient impairment* = At least two components are affected, no complete failures and no complete impairment. At least one component is working.

Table 3.5 presents the resulting multi-unit event severity per multi-unit classification factor and component type.

Table 3.5. Multi-unit event severity per multi-unit classification factor and component type

Component type	Multi-unit event severity					Total	[%]
	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment		
1. Internal factors – shared cause	**4**	**17**	**7**	**26**	**3**	**57**	**66%**
Battery		1		5	1	7	8%
Centrifugal pumps	2	6		7	1	16	18%
Check valves		3		1		4	5%
Diesels		4	6	5	1	16	18%
Heat exchanger		1		1		2	2%
Level measurement				1		1	1%
Motor operated valves	1	2	1			4	5%
Safety and relief valves	1			6		7	8%
2. External factors – Shared environment or physical connection	**4**	**3**	**1**	**5**	**1**	**14**	**16%**
Breakers		1				1	1%
Centrifugal pumps	3	1				4	5%
Control rod drive assembly		1				1	1%
Diesels	1		1	5		7	8%
Motor operated valves					1	1	1%
3. Fleet CCF events	**1**	**6**	**2**	**4**	**3**	**16**	**18%**
Battery		2				2	2%
Breakers			1			1	1%
Centrifugal pumps				1	1	2	2%

Component type	Multi-unit event severity					Total	[%]
	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment		
Check valves		1				1	1%
Diesels		1	1		1	3	3%
Level measurement	1	1		1		3	3%
Motor operated valves				1		1	1%
Safety and relief valves		1		1	1	3	3%
Total	**9**	**26**	**10**	**35**	**7**	**87**	**100%**

4. Overview of multi-unit event database content

This chapter presents an overview of the data set, which includes 87 multi-unit events. It includes tables with the event parameters, i.e. event cause, coupling factor, detection method, CCF root cause, corrective action and event severity. The event parameters are defined in the ICDE general coding guidelines (NEA, 2011), see Annex 1.C. The conclusions drawn from the overview of the data of the multi-unit events are that:

- The most common component types among the multi-unit events were diesel (30%) and centrifugal pumps (25%), followed by safety relief valves (11%) and batteries (10%).
- The most common multi-unit event severities[3] were "complete impairment" (39%), followed by "partial CCF" (31%). Nine events were complete multi-unit CCFs (10%).
- The most common event causes were "design, manufacture or construction inadequacy" (40%) followed by "procedure inadequacy" (20%), "internal to component, piece part" (13%), and "abnormal environmental stress" (9%).
- The most common coupling factor was "hardware" (52%) followed by "operational" (33%) and environmental (15%).
- No particularly common detection method was observed. About 10% of the events were events by demand. However, many differences and no consistent coding among the ICDE events within multi-unit events was observed.
- "Design modifications" (26%) followed by "specific maintenance/operation practices" (22%) and "general administrative/procedure controls" (17%) were the most common corrective actions.

By combining the coded information for the (apparent) event causes (ECs), the corrective actions (CAs) and the coupling factor (CF), insights regarding the CCF root cause of the multi-unit events can be gained. The following conclusions can be drawn:

- The most common CCF root cause for multi-unit CCF events is a deficiency in the design of components and systems; while events due to design-related issues cause already nearly 50% of all events in the ICDE database, the relative share of the multi-unit events is nearly 60%.
- Events with the CCF root cause "predominant design and environment" are significantly overrepresented compared to other events in the ICDE database. This is an indication that multi-unit events which involve environmental effects usually require design improvements to prevent reoccurrence.

3. The multi-unit event severity is a combination of the ICDE events component impairment vectors, see Section 3.2.3.

- Human actions as CCF root cause (solely or predominant) are underrepresented compared to other events in the ICDE database, though the statistical basis is weak.

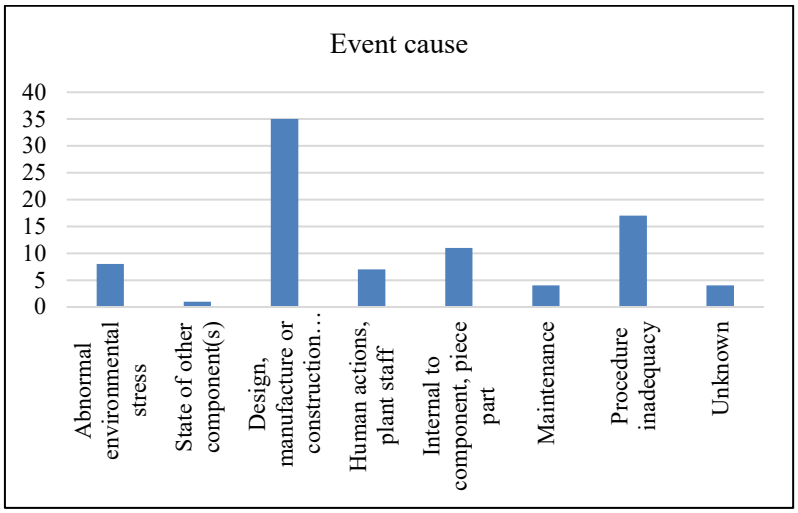
4.1 Event cause (apparent cause)

Table 4.1 and Figure 4.1 present the distribution of the apparent event causes. For a couple of events within the multi-unit events, the coding of the event cause is not the same and has a small impact on the statistics.

Table 4.1. Distribution of event causes

	Multi-unit event severity						
Event cause	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	**Total**	**[%]**
Abnormal environmental stress	3	2	1	2		8	9%
State of other component(s)		1				1	1%
Design, manufacture or construction inadequacy	3	13	3	11	5	35	40%
Human actions, plant staff		1	2	4		7	8%
Internal to component, piece part		5	1	5		11	13%
Maintenance		1	1	2		4	5%
Procedure inadequacy	3	2	2	8	2	17	20%
Unknown		1		3		4	5%
Total	**9**	**26**	**10**	**35**	**7**	**87**	**100%**

Figure 4.1. Distribution of event causes



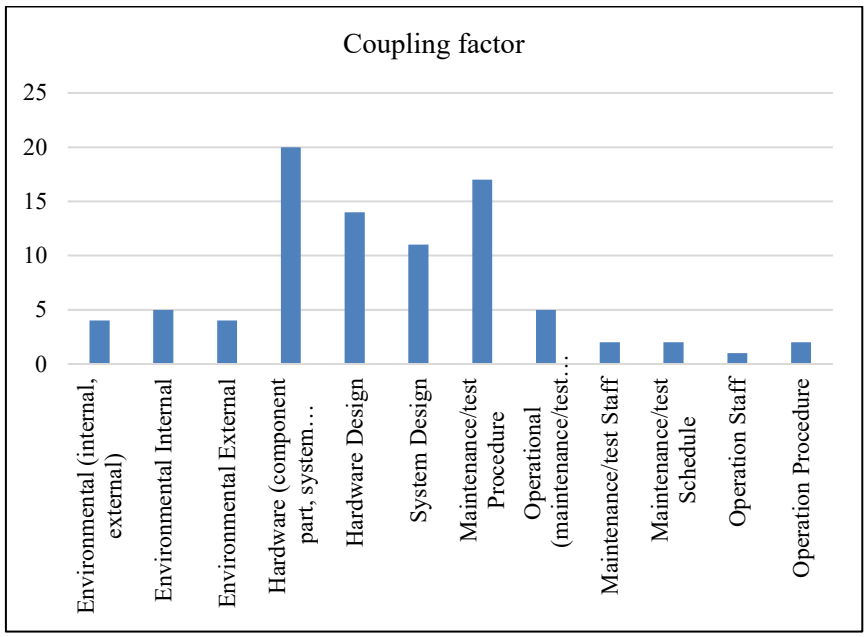
4.2 Coupling factor

Table 4.2 and Figure 4.2 present the distribution of coupling factors. The coupling factor describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected. The coding of coupling factor differs for a couple of events within the multi-unit events, though this has a small impact on the statistics.

Table 4.2. Distribution of coupling factors

	Multi-unit event severity						
Coupling factor	Complete CCF	Partial CCF	CCF Impaired	Complete impairment	Incipient impairment	**Total**	**[%]**
Environmental	**1**	**2**	**1**	**9**		**13**	**15%**
Environmental (internal, external)		1		3		4	5%
Environmental internal	1	1		3		5	6%
Environmental external			1	3		4	5%
Hardware	**5**	**19**	**4**	**13**	**4**	**45**	**52%**
Hardware	2	7	3	6	2	20	23%
Hardware design	1	7	1	4	1	14	16%
System design	2	5		3	1	11	13%
Operational	**3**	**5**	**5**	**13**	**3**	**29**	**33%**
Operational			3	2		5	6%
Operation staff		1				1	1%
Maintenance/test procedure	2	4	1	8	2	17	20%
Maintenance/test schedule			1	1		2	2%
Maintenance/test staff				1	1	2	2%
Operation procedure	1			1		2	2%
Total	**9**	**26**	**10**	**35**	**7**	**87**	**100%**

Figure 4.2. Distribution of coupling factors



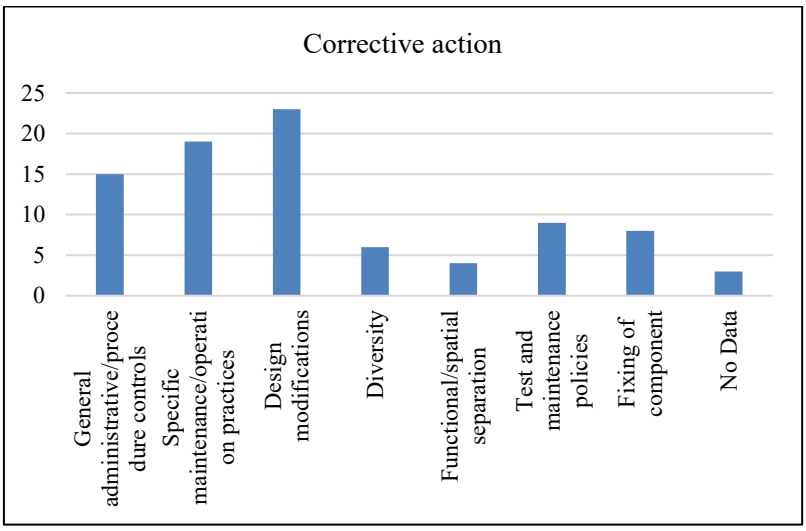
4.3 Corrective action

Table 4.3 and Figure 4.3 present the distribution of corrective actions. The coding of the corrective actions differs for a couple of events within the multi-unit events, but this has a small impact on the statistics.

Table 4.3. Distribution of corrective actions

	Multi-unit event severity						
Corrective action	Complete CCF	Partial CCF	CCF impaired	Complete impairment	Incipient impairment	**Total**	**[%]**
General administrative/procedure controls	2	3	4	4	2	15	17%
Specific maintenance/operation practices	3	4	3	9		19	22%
Design modifications	3	8	1	9	2	23	26%
Diversity		4	1	1		6	7%
Functional/spatial separation	1	1		2		4	5%
Test and maintenance policies		2		6	1	9	10%
Fixing of component		3		3	2	8	9%
No data		1	1	1		3	3%
Total	**9**	**26**	**10**	**35**	**7**	**87**	**100%**

Figure 4.3. Distribution of corrective actions



4.4 CCF root cause

The root cause is "the most fundamental reason for an event or adverse condition, which if corrected will effectively prevent or minimise recurrence of the event or condition."[4]

By combining the coded information for the (apparent) event causes (ECs) the corrective actions (CAs) and the coupling factor (CF) insights regarding the CCF root causes of the multi-unit 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:

- deficiencies in the design of components or systems (design);
- procedural or organisational deficiencies (procedures);
- deficiencies in human actions (human actions).

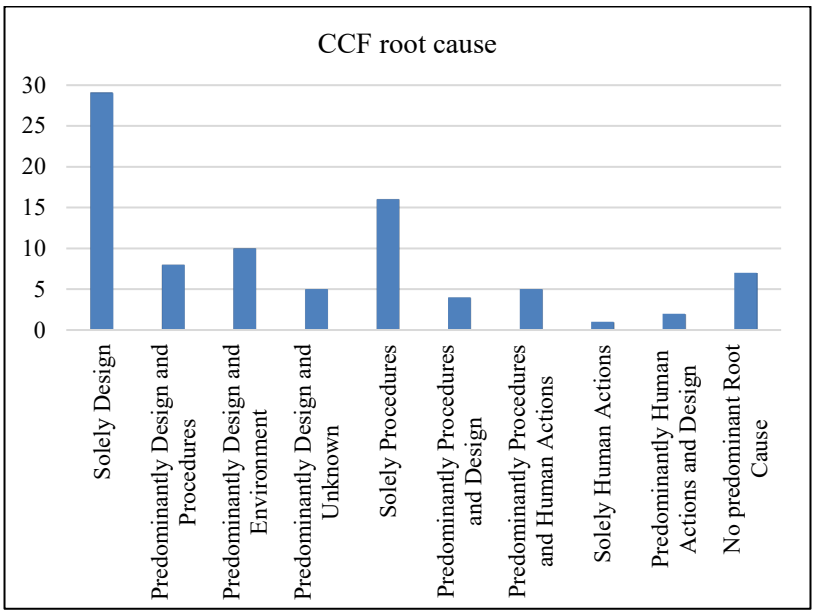
In addition to these three basic aspects, the supporting aspects "environmental" and "unknown" are used in case events due to external factors or events which are not completely coded. It is noted if all three aspects of an event are identical (e.g. 3 x design) or if there is a predominant and a contributing CCF 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 4.4.

4. See IAEA-TECDOC-1756 for more details.

Table 4.4. Distribution of CCF root causes

	Multi-unit event severity						
CCF root cause	Complete CCF	Partial CCF	CCF impaired	Complete impairment	Incipient impairment	Total	[%]
Solely and predominantly design	**6**	**20**	**4**	**18**	**4**	**52**	**60%**
Solely design	2	15	2	8	2	29	33%
Predominantly design and procedures	1	1	1	3	2	8	9%
Predominantly design and environment	3	2		5		10	11%
predominantly design and unknown		2	1	2		5	6%
Solely and predominantly procedures	**3**	**4**	**5**	**11**	**2**	**25**	**29%**
Solely procedures	3	3	2	7	1	16	18%
Predominantly procedures and design		1	1	1	1	4	5%
Predominantly procedures and human actions			2	3		5	6%
Solely and predominantly human actions		**1**		**1**	**1**	**3**	3%
Solely human actions				1		1	1%
Predominantly human actions and design		1			1	2	2%
No predominant CCF root cause		**1**	**1**	**5**		**7**	**8%**
Total	**9**	**26**	**10**	**35**	**7**	**87**	**100%**

Figure 4.4. Distribution of CCF root causes



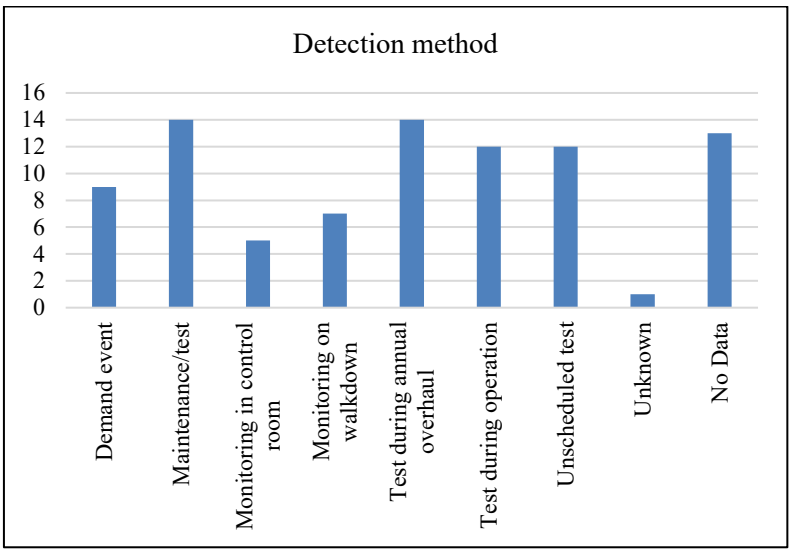
4.5 Detection method

Table 4.5 and Figure 4.5 present the distribution of detection methods. For many events within the multi-unit events, the coding of detection method differs and has a large impact on the statistics.

Table 4.5. Distribution of detection methods

	Multi-unit event severity						
Detection method	Complete CCF	Partial CCF	CCF impaired	Complete impairment	Incipient impairment	**Total**	**[%]**
Demand event	4	4	1			9	10%
Maintenance/test		3	2	9		14	16%
Monitoring in control room		2		3		5	6%
Monitoring on walkdown		1		6		7	8%
Test during annual overhaul	2	6	1	4	1	14	16%
Test during operation	2	4	2	3	1	12	14%
Unscheduled test	1	1		6	4	12	14%
Unknown				1		1	1%
No data		5	4	3	1	13	15%
Total	**9**	**26**	**10**	**35**	**7**	**87**	**100%**

Figure 4.5. Distribution of detection methods



5. Engineering aspects of collected multi-unit events

This chapter presents the engineering aspects of the analysed multi-unit events. The analysis was performed according to the workshop form in Annex 1.E. For each multi-unit event, the following was analysed:

- correlation factor – multi-unit event dependency;
- plant state when the events were detected;
- failure mechanism descriptions;
- marking of interesting events;
- actual defences that prevented all components from failing (if not a complete CCF);
- areas of improvements to prevent the event from happening again.

5.1 Correlation factor between multi-unit events

In the analysis, the type of correlation factor (multi-unit event dependency) between the events was identified. Table 5.1 presents the identified correlation factors and the internal factors dominate the results (84%). The correlation factors and sub-factors were identified by the ICDE steering group members during the data analysis workshops. A single correlation factor and single sub-factor was identified for most events; however, more than one sub-factor was identified for 11 of the 87 multi-unit events. The correlation factors and sub-factors are defined in the workshop form, as shown in Table 1.E.1 in Annex 1.E.

Table 5.1. Correlation factors between multi-unit events

Multi-unit event correlation factors	Site event	Fleet event	Number of multi-unit events	Percentage
Internal factors	**57**	**16**	**73**	**84%**
Organisational	17	2	19	22%
Human	7		7	8%
Identical design	27	13	40	46%
human and organisational	1		1	1%
identical design and organisational	4	1	5	6%
identical design and human	1		1	1%
External factors	**14**	**0**	**14**	**16%**
Shared SSCs	7		7	8%
Proximity	3		3	3%
Shared SS's and identical design	1		1	1%
Shared SSCs and proximity	1		1	1%
Shared SSCs and human	1		1	1%
Proximity and human	1		1	1%
Total	**71**	**16**	**87**	**100%**

5.1.1 Internal correlation sub-factors

For the internal correlation factor events, the dependencies involve *"organisational", "human"* and *"identical design".* All the identified fleet CCF events were correlated by internal factors.

- *Organisational*

  The events assigned to the "organisational" factor concern mainly incorrect procedures (both test and maintenance), possible latent design issues, ageing, non-conservative design practices, and not meeting design load requirements.

- *Human*

  Events correlated by "human" factors involve issues with maintenance actions, such as cleaning (grease) and improper fixing.

- *Identical design*

  The events assigned to "identical design" factors are correlated through the same design of components/systems, operating environment, or installation. Also, some events are correlated by the use of the same unsuitable grease/lubrication.

5.1.2 External correlation sub-factors

A total of 14 events were characterised by external correlation sub-factors. Of the external factor events, four were identified with two sub-factors. In three events the second identified sub-factor was an internal correlation sub-factor. In these events, it appeared that both external and internal factors contributed to the dependency. The external factors involve "*shared SSCs"* and "*proximity."*

- *Shared SSCs*

  The events assigned to this sub-factor involve shared systems, structures or components between the units, such as shared diesels between the units, connected supply lines (piping), and common fuel storage tank. Ten external factor events are correlated to "shared SSCs."

- *Proximity*

  The events assigned to this sub-factor involve correlations related to the site location, site layout or a shared dependency external to the site. Examples include area events or external events. Examples of shared external dependency are a shared cooling water source or a common dependency on the electrical grid. The four events assigned to the factor "proximity" involve a shared cooling water intake channel, weather conditions (snow with strong winds) and a shared control room.

5.2 Plant state when the events were detected

This engineering review provides information about the plant state when the multi-unit events were detected. This information may be useful to develop insight into detection methods and the safety significance of multi-unit events. For example, events occurring when both/all units are at full power may have a higher safety significance. Many of the

events occurred/were detected during different plant states or at both/all units at full power. Table 5.2 presents the statistics for the plant states when the events were detected, grouped by internal/external correlation factors. For the external factor events, about 50% were detected at both/all units at full power.

Table 5.2. Plant state when the events were detected per internal/external correlation factors

Plant states when detected	Internal factors	External factors	Number of multi-unit events	Percentage
Different plant states	30	7	37	43%
Full power (both/all units)	12	6	18	21%
Start-up (both/all units)	1		1	1%
Shutdown (both/all units)	2		2	2%
Outage (both/all units)	11		11	13%
Unknown (both/all units)	17	1	18	21%
Total	**73**	**14**	**87**	**100%**

5.3 Interesting events – discussion and examples

The marking of 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. An event can be applied to several codes. Table 5.3 presents the statistics per interesting event code.

Table 5.3. Applied interesting event codes

Interesting CCF event code	Description ***Purpose***	No. of events
Complete CCF (1)	Event led to a complete CCF. *This code sums up all complete CCFs, for any component type.*	9
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.*	11
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 safety function during the mission time.*	5
Multiple defences failed (4)	Several lines of defence failed *More than one line of defence against CCF failed, e.g. in the quality assurance (QA) processes of designer, manufacturer, technical support organisation (TSO) and utility during construction and installation of a set of components.*	2

Interesting CCF event code	Description ***Purpose***	No. of events
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).*	7
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.*	3
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.*	6
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.*	87
Total marks		**130**

- Complete CCF: The complete CCF events are further discussed in Section 5.4.
- CCF outside planned test: A total of 11 multi-unit events were detected outside normal periodic and planned testing and inspections. The events were detected by special test, unplanned control, audit, and via experience feedback from another unit. All events had an internal correlation factor.
- Component not capable: Five multi-unit events were assessed to be incapable of performing their safety function over a long period of time. The events reveal installation deficiencies and lack of consideration of all accident or abnormal operating conditions that may occur. All five events had an internal correlation factor.
- Multiple defences failed: Two events were assessed to have had multiple defences fail. One event involved SRVs that were incorrectly refurbished by the plant operator and manufacturer, in addition to an incomplete test technique used by the manufacturer. This event shows failure in the QA process of both the manufacturer and plant. Both events had an internal correlation factor.
- Multiple systems affected: Seven multi-unit events had an intersystem dependency, i.e. indications that factors affected other systems/functions. Four of the events were attributed to external correlation factors, such as problems at water intake affecting cooling in other systems.

- Common-cause initiator: Two of the three events marked with this code were complete CCFs and concerned problems with the water intake (external correlation factor).
- Safety culture: Six events were assigned the safety culture code. Examples of observed problems involve confusion between pressure units in calibrating set points, erroneously interchanged gauge lines (level measurement) during plant construction, and use of unsuitable grease. These events demonstrate a lack of careful attention to detail and inadequate training and/or procedures. Suggested improvements to prevent such events from happening again involve updated procedures and improved management systems. All six events had an internal correlation factor.

5.4 Lessons learnt from complete CCFs

The engineering analysis identified actual CCF defences that were present in the events and possible improvements to defences. The defences should be considered as preventions against the failure of all components 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 from happening again. The actual defences observed in non-complete CCFs are discussed in Section 5.5. Each possible defence is assigned to one of the categories given in the workshop form, as shown in Appendix E.

Nine multi-unit events were complete CCFs and possible defences and/or areas of improvement were identified for these events. “Improved design of system” was assigned to four events, and “improved surveillance/maintenance” was assigned to four events. Five events had an internal correlation factor and four events had an external correlation factor. In the following sections, the identified improvements for complete CCF events are presented according to the internal/external factors.

5.4.1 Complete CCF possible defences for internal factors

Below is a description of the internal factor events and the identified improvements:

- In an event at a twin unit site, wrong settings for safety relief valves were detected at two groups of valves, one in each unit. The reason for the wrong settings was incorrect engineering judgement and identical maintenance actions applied for all valves, resulting in a complete CCF (correlation factor: human and organisation) of two groups of safety valves. As defence, it was proposed that a process be introduced to ensure the completeness, quality and validity of maintenance procedures, e.g. by an independent verification of the used input data and calculations.
- In another event, the limit switch of multiple level measurements failed to trigger on demand because of an inadequate position of the nozzles for level measurement, which resulted in the level being indicated too high (correlation factor; identical design). The event was a complete CCF detected outside planned tests and the components were not capable of performing their required functions. This design failure was present at multiple nuclear power plant units of the same type. The event led to design modifications, with re-installations at the correct position for low-level measurements. Tests under real demand conditions would have revealed the

problem. As a defence, a change of testing procedures (consequent use of real demand testing whenever possible) was suggested.

- At an event at a twin unit site, high temperatures and low levels in the suction source tank led to unexpected cavitation of two out of two pumps at each unit. The conditions at the suction side of the pumps (low net positive suction head [NPSH]) were not foreseen due to errors in the design calculations. As an improvement, a revision of the system design and more comprehensive test procedures were proposed. The multi-unit correlation factor was "identical design".
- An event at a twin unit site saw erroneous start permissive interlocks at lube oil pumps at the auxiliary feed-water pumps resulting from design errors implemented during plant modifications. The design error removed a start permissive interlock contact affecting the time delay on low oil pressure causing a trip on low oil pressure at the start of the pumps (correlation factor; identical design). As an improvement, design modifications were implemented.
- At an event at a twin unit site, design modifications to the logic of the containment isolations were erroneously not applied on-site to a group of motor-operated valves in the residual heat removal system in each of the two plants. Because of this, containment isolation would not have been available in the plant shut down phase for this system as required in the technical specifications. The multi-unit correlation factor was organisation. Diverse maintenance teams would increase the possibility to identify such failures.

5.4.2 Complete CCF possible defences for external factors

For the external factor events, the following improvements were identified:

- At three events the availability of the (essential) service water intakes was endangered by foreign material (fish, ice, etc.) blocking the intake screen. Better design of water intake (such as cleaning of strainers, adding back-flushing capability, etc.) could prevent the events from happening again. These events' multi-unit correlation factor was "shared SSCs".
- At an event at a twin unit site, the service water pumps of both units became air bound (correlation factor was "shared SSCs"). Underwater diving maintenance activities were identified as the source of the air. As defence, it was proposed to change the maintenance procedure.

5.5 Lessons learnt from actual observed defences

For the non-complete CCF events, the task was to identify actual defences. An actual defence is a defence that prevented the event from becoming more severe, i.e. it prevented all components from failing. Each actual defence should be assigned to one of the categories given in the workshop form in Annex 1.E. In Table 5.4 the most common actual defence categories are "surveillance/maintenance" of component (c) and "testing procedure" (d) and mainly correlated through internal multi-unit factors. In the following sections, the actual defences are presented according to the internal/external factors.

Table 5.4. Actual defences for non-complete CCF events

Actual defences	Internal factors	External factors	Number of multi-unit events	Percentage
Design of system or site (a)	1	1	2	3%
Design of component (b)		1	1	1%
Surveillance/maintenance, etc. (c)	**19**	**3**	**22**	**28%**
C	15	2	17	22%
c, d	3		3	4%
c, f	1		1	1%
Testing procedure (d)	20	1	21	27%
Operation procedure for component (e)	1		1	1%
Management system of plant (f)	3	2	5	6%
No defence identified	13	2	15	19%
Demand event, just luck?	1		1	1%
Slow developing failure mechanism	9	1	10	13%
Total	**68**	**10**	**78**	**100%**

5.5.1 Actual defences observed for internal factors

A total of 19 events were assigned to the category "surveillance of component or maintenance procedure for component". Monthly surveillance and verification of operability detected the problems. Also, inspections (from other unit/site) led to detection in time and maintenance was sufficient to detect the problems.

Another important category for defence was "testing procedure". Many events were prevented by routine, periodic or annual testing. For a few events, special testing (due to unknown reasons) revealed the problem. Nothing specific regarding testing was identified and ordinary testing procedures were sufficient to detect the problems before they developed into more severe failures.

For the category "management system of plant", the observed actual defences highlight the importance of operating experience feedback, especially for the multi-unit events where the feedback led to inspections at other units. Also, audits and other types of analysis are observed defences that prevented all components from failing. For nine events, the failures developed slowly over time and could be detected. For 13 events, no actual defence could be identified.

The identified actual defences that kept events from developing into complete CCFs include adequate test and maintenance procedures and inspections. Also, some failures developed slowly over time and could be detected before developing into complete CCFs. Thus, feasible defence strategies against failures developing into complete CCFs include having well-functioning testing procedures, maintenance procedures, operating experience feedback, skilled personnel, etc.

Based on the distribution of complete CCFs and incomplete CCFs, it can be concluded that adequate defences exist for most of the events. Also, only 10% of the events were detected by demand (see Table 4.5), and this is probably because most events are not failures on demand but failures detected by surveillance, maintenance or testing. Thus, adequate and robust system/component design is the fundamental defence against complete CCFs.

5.5.2 *Actual defences observed for external factors*

Ten non-complete CCF events were external factor events. For one event, the design of the system was sufficient to cope with the failure mechanism (sludge in the cooling water system), and the testing was sufficient to discover the failure early enough. For another event, the design of the filters was sufficient to cope with the failure mechanism. Also, surveillance during maintenance and local checks revealed the problems for some events. For another event, the failure had slowly developed over time and was detected during maintenance activity before all components failed. For two events, no actual successful defence could be identified, and for another two events no clear defence was identified.

5.6 Areas of improvement

For the non-complete CCF events, the task was also to identify areas of improvement. An area of improvement aims to identify what to improve 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 5.5 presents the areas of improvement per multi-unit event correlation, i.e. internal/external factor. The following section presents improvements per internal and external correlation factor. Events marked with an asterisk (*) are fleet CCF events.

Table 5.5. Non-complete CCF areas of improvement per multi-unit event correlation

Non-complete CCF – Areas of improvement	Internal factor	External factor	Total	Percentage
a) Design of system or site	8	6	14	13%
b) Design of component	24	2	26	24%
c) Surveillance of component or Maintenance procedure for component	20	4	24	22%
d) Testing procedure	21	1	22	21%
e) Operation procedure for component	2	0	2	2%
f) Management system of plant (QA of vendor, spare parts management, training of personnel, sufficient resources/staff, etc.)	16	3	19	18%
Total	**91**	**16**	**107**	**100%**

5.6.1 *Areas of improvement for internal factors*

Design of system or site

Events for which the category *design of system or site* was suggested as an improvement are presented below. The component type is given in parentheses, if needed.

Failure mechanism

- Temperature and pressure fluctuations due to problems with controlling the water flow to the oil coolers caused two pumps to trip.

Improvement – Design of system

- Oil cooler to be fitted with new control system and valve.

Failure mechanism	Improvement – Design of system
● In case of short circuit in the DC system, the fault current may destroy the switchgear because new batteries, which had been installed as part of a plant modification, led to a higher short circuit current than designed for.	➢ Design of system.
● *Faults in the I&C logic not taking into account all possible accident conditions caused multiple motor operated valves to not open completely under these conditions.	➢ Design of system.
● Insufficient water level in suction pond may have caused several pumps to trip. This behaviour was not considered in the design.	➢ Design of system.
● System design inadequacy led to implementation of undersized batteries in several units.	➢ Design of system.
● A wiring error in the EDG control panel lead to a too high increase of diesel power when grid voltage gradually increased during a 24-hour run test.	➢ System design and QA of component.
● Multiple defective relays (faulty relay contact operating mechanism) caused several pumps to trip.	➢ Design of system and testing.
● Batteries were not capable of supplying required loads by design error. During testing it was never attempted to operate with a single battery bank as required by the technical specifications.	➢ Design of system and testing procedure. An appropriate testing procedure did not exist.

Design of component

For the events in which design of component could prevent the events from happing again, a general improvement of component design without any specific details was commonly suggested. Example of events with specific design improvements of components are presented below.

Failure mechanism	Improvement – Design of component
● Drifted lift pressures of SRVs led to two valves being outside the operating rule limit.	➢ Modification of valve set points.

Failure mechanism	Improvement – Design of component
● *Early ageing of the lubricant, leading to increased opening times of several breakers.	➢ Consider ageing.
● Erosion/corrosion degrades flow dividing plate of several heat exchangers.	➢ Better material.
● Inappropriate supporting structures (clamps) in combination with vibrations while running EDG caused cracks in fuel supply system.	➢ Modification of clamp design.
● Several MOVs failed or were degraded because of fatigue type cracks at bakelite pinions which are part of the valves actuator.	➢ Using brass instead of bakelite for pinions.
● Temperature control channel malfunction led to the potential unavailability of thermostatic three-way valves in the cooling system of the EDGs.	➢ Readjust the three-way valve temperature control channels.
● *Thermostatic three-way valve incipient failure due to valve/rod anti-rotation pin failure but without valve/rod assembly unscrewing (EDG).	➢ Better design and quality of component.
● Vibrations loosened the connector of thermo couples in the EDGs exhaust gas system and caused inadvertent trips at high exhaust gas temperature (a trip signal only in normal mode, not in emergency mode). (EDG).	➢ Design modification (removed signal).
● Cracks in numerous relay sockets induced by vibrations in the EDG rooms could result in failure of diesel load control.	➢ Better design of the relay sockets. Diverse diesel generators. More frequent maintenance would have detected the event earlier.
● Due to unclear specifications, several relays of the I&C of several pumps were not installed appropriately, leading to the potential failure of several pumps in case of a demand event.	➢ Use the same material and ensure adequacy between material and maintenance.
● Shear of hold-down bolts due to vibration affecting several pumps.	➢ Improve pump anchorage and consider visual inspections.
● Cracking of cell top due to positive pillar corrosion affecting several batteries.	➢ Improve the design of the positive pillar to avoid corrosion. Consider the ageing effect and introducing environmental tests to ensure the component will withstand the requirements.

Failure mechanism	Improvement – Design of component
● Loss of storage capacity of several batteries due to carbonation of positive plate because inadequate materials were used.	➢ Improve the design of the plate to avoid the carbonation and select a right material. Consider the ageing effect and the introduction of environmental tests to ensure the component will withstand the requirements.

Surveillance of component or maintenance procedure for component

For the events assigned to this area of improvement, the events concerned:

- improvement of inspections or surveillance of the component groups;
- specific improvements of maintenance;
- improvements of the QA of maintenance and revision of maintenance programme; and
- an updated/improved maintenance procedure in general.

Examples of such events are:

Failure mechanism	Improvement – Surveillance/maintenance
● Tube sheet blockage due to corrosion products potentially impaired the function of multiple EDG coolers.	➢ Surveillance of component (maybe the problem could have been identified earlier).
● Two cooling pumps failed due to human errors resulting from unclear work orders and communication problems.	➢ Make judgement prior to maintenance if other redundancies can be affected.
● Two check valves stuck open because of the presence of oxide deposit.	➢ Introduce a process to ensure completeness, quality and validity of maintenance procedures.
● Bearings of two pumps were impaired because of degraded bearing oil. Reason for the degraded oil was ingress of foreign material into the oil.	➢ Improving maintenance procedures (quality of oil).
● Mixture of incompatible greases affected bearings of several pumps and pump motors.	➢ Updating maintenance procedures.
● Reduced flow caused by clogging/macrofouling due to inadequate cleaning of HE tubes. Testing, surveillance and trend observation was not adequate to detect the failure in time.	➢ An enhanced inspection and maintenance programme.

Failure mechanism	Improvement – Surveillance/maintenance
● Incomplete cleaning procedure leading to temporary cleaning filters being erroneously left in the suction line of the AFWS pumps.	➢ QA of procedure (checking the completeness of the procedure).
● Inadequate maintenance procedure leading to disk misalignment in check valves and therefore leakage.	➢ QA procedure (checking in detail the procedure so that the absence of acceptance criteria would have been pointed out).

Testing procedure

Some of the events concern improvements related to testing requirements, e.g. to ensure that the test procedure confirms the components' functional requirements. A few events concern improvements for post-testing, often after a modification. For the remaining events in this category, an updated or improved test procedure was suggested. For testing, it is important to have a good QA of the procedure to ensure that all requirements are met and that the procedure is sufficient. As seen in Section 5.4.1, it is important to have well-functioning procedures to be able to detect the events in time before they develop into complete failures. Examples of events in this category are:

Failure mechanism	Improvement – Testing procedure
● Batteries were not capable of supplying required loads by design error. During testing it was never attempted to operate with a single battery bank as required by the technical specifications.	➢ Design of system and testing procedure. An appropriate testing procedure did not exist.
● *High temperature caused gumming-up of the lubricant and the subsequent jamming of multiple motor operated safety and relief valves.	➢ Test the new lubricant under right conditions.
● *Level transmitters did not match the functional criteria (cause unknown), but could probably be due to incorrect installation (mounted at wrong positions).	➢ Checking of signals to comply with requirements.
● Insufficient charging of batteries.	➢ Improve procedures for the operation (charging) and surveillance of the batteries.
● Fuel injection pumps at multiple EDGs broke because of screws rupturing due to improper fixing.	➢ Post-testing of component.
● Several MOVs were found with wrong torque limit switch settings, which might cause them not to open on demand. The wrong torque limit settings were applied during modification activities.	➢ Modification of test procedure (include post-modification test).

Failure mechanism	Improvement – Testing procedure
● Use of an outdated procedure, including an outdated measurement scale, led to the miscalibration of several level measurement transmitters.	➢ Avoid re-use of faulty procedure.
● Check valves were sticking because of corrosion.	➢ Shorter test intervals.

Operation procedure of component

Only two events were assigned to this category.

Failure mechanism	Improvement – Operation procedure of component
● Inadequate manufacturing tolerances resulted in sticking of air valve pistons at multiple EDGs.	➢ Not to operate cross-connected.
● Magnetic pickup target gear shaft (part of the EDGs rpm sensors) failed during load test. A manufacturer defect in the shaft caused the failure. The same component was installed on other EDGs at the site.	➢ Operation procedure.

Management system of plant

Some of the events in this category concern improvements of different QA parts of the management system of plant. A few events concerned specific improvements of management system of plant. For the remaining events assigned to this category, no specific improvement was suggested. Examples of events in this category are:

Failure mechanism	Improvement – Management system of plant
● Inadequate manufacturing tolerances resulted in sticking of air valve pistons at multiple EDGs.	➢ QA of vendor.
● Magnetic pickup target gear shaft (part of the EDGs rpm sensors) failed during load test. A manufacturer defect in the shaft caused the failure. The same component was installed on other EDGs at the site.	➢ QA of vendor.

Failure mechanism	Improvement – Management system of plant
● Confusion between pressure units led to the SRV's settings not complying with operating rule.	➢ Process to ensure completeness, quality and validity of tests.
● *Erroneously interchanged level measurement gauge lines during plant construction led to freezing of the accumulator low-level measurement signal so that this signal could not be triggered when the level in the accumulator fell below this limit. This could not be detected because the accumulators are not emptied during normal testing.	➢ Better QA during construction.
● Shearing of motor pinion keys of multiple MOVs due to improper material.	➢ QA of management.
● *Use of unsuitable grease at several pumps after the manufacturer stopped the production of the formerly used grease.	➢ Spare parts management. Qualification of replacement of grease.
● Incorrect re-assembly following SRV refurbishment and incomplete testing led to a degraded discharge capacity of several SRVs.	➢ Refurbishment quality improvement by manufacturer and by the plant.
● * Use of improper pump motor connectors at several pumps. In case of loss-of-coolant accident (LOCA) or steam pipe rupture, the generated steam would have created a short circuit in the connectors that could have led to a failure of the pumps.	➢ Perform inspections during plant construction.
● The wrong type of relays in the motor starters of several pumps had the potential to cause the pumps to run at reduced speeds.	➢ Spare parts management.
● *Fatigue cracks on diesel engine parts (con-rods) due to design errors at the piece parts.	➢ The manufacturer decided to change the design after the utility discovered the cracks. The utility should have better oversight of the manufacturer.
● *Use of grease that was not qualified for accident condition temperatures at several MOVs.	➢ Better training and surveillance of manufacturer staff (should be aware of the importance of specifications for grease).

Failure mechanism	Improvement – Management system of plant
● Failure of resistors in the governor unit of multiple EDGs could have led to speed oscillations. The resistors failed due to long term heat fatigue.	➢ Increase replacement frequency.

5.6.2 Areas of improvement for external factors

For the multi-unit events with correlation factor *"external"*, the most common assigned areas of improvement were "design of system or site" and "surveillance/maintenance".

Proximity

Failure mechanism	Improvement
● Sludge movement in the sea water channel led to reduced heat capacity of sea water heat exchangers of multiple EDGs.	➢ Mussel strainers were installed.
● Slight leaks at cooling pipes of multiple EDGs due to external corrosion due to rainwater penetration in the EDG building. The water had accumulated between the cooling pipes and the insulating sleeves.	➢ Make the EDG building leak-proof and surveillance of the roof.
● Human error due to distractions while performing control rod movements led to wrong control rod positions in several units.	➢ Design of system by separating the control rooms and training of personnel; diversify the operators between the units.
● Unusual weather conditions, with dense snowing and high wind speed in the direction of the walls, caused partial blocking of the combustion air filters at several EDGs.	➢ Design modifications and, in case they are not enough, a procedure to remove the air filter in case of snow blockage.

Shared SSCs

Failure mechanism	Improvement
● Air trapped in the governor compensation system caused vibrations and resulted in operating in a degraded state. (EDG).	➢ Introduce diversity (system design).
● Design error resulted in ice plug in backwash line. (MOV).	➢ Design of system.
● Passing of the non-return valve led to a reverse flow through the pumps and the pumps tripped on high temperature.	➢ System design, better maintenance planning and failure detection.
● Wiring error of the under voltage-monitoring of breakers caused them not to close as designed.	➢ Design of component.
● Wrong calibration of fuel storage tank level could have led to unavailability of several EDGs.	➢ Better surveillance of the level measurement in the common tank.
● Sandblast cleaning of the combustion air intercoolers caused sand to be introduced into the engines and then scoring of cylinder liners and piston rings at multiple EDGs.	➢ Maintenance cleaning procedure and upgrade of QA work plan.

5.7 Candidates for MUPSA modelling

The criteria defined in Section 3 have been used to identify candidate events and component groups for multi-unit PSA (MUPSA) modelling. A total of 14 multi-unit events were identified to have a shared environment or physical connection, i.e. events correlated by external factors. These events are presented in Sections 5.4.2, 5.5.2 and 5.6.2.

It is expected that if the single unit PSA is extended to a MUPSA, the physical connections and dependencies across unit boundaries will be accounted for and explicitly modelled. Also, the external factor aspects identified in 5.1.2 should be considered.

The assessment of external factors can involve identifying the shared SSCs that can introduce CCF dependencies at the site, and identifying any external dependencies related to the site location or proximity, e.g. shared environmental conditions, shared electrical grid dependency.

A total of 57 multi-unit events were assessed as *dependent multiple events at a site with a shared cause*, i.e. internal factors. For these events, new CCF groups may need to be defined in a MUPSA to combine common-cause component groups across all units at the site. Also, the internal factor aspects identified in 5.1.1 should be considered.

The assessment of internal factors can involve identifying the organisational, human and design-related aspects that can introduce CCF dependencies. Consider what defences exist in these areas and where defences can be improved. These considerations can assist in identifying and developing the site-level CCF groups that may be needed for MUPSA.

6. Summary and conclusions

This report summarises the results of two data analysis workshops performed by the ICDE steering group to evaluate multi-unit CCF events. The workshops covered 87 multi-unit events involving 192 ICDE events affecting multiple units at one or several sites. The goal was to analyse these types of events by identifying multi-unit dependencies and CCF defence aspects related to such events.

These reported ICDE events were classified with respect to: degree of multi-unit correlation expressed by internal and external correlation factors; simultaneity between the events; degree of severity; and whether the events occurred at different plant sites. The observed multi-unit events were classified as:

- **Internal factors:** These CCF events involve two or more reactor units located at the same site. The shared cause of the component failures involves the design of systems and components, maintenance procedure or other organisational factors that are common between the multiple units.
- **External factors:** These CCF events involve two or more reactor units located at the same site. There exists a physical connection, an external connection or a shared external environment between the affected systems and components.
- **Fleet CCF events:** These events involve the same or similar types of CCF events that occur at different sites.

The analysis included an assessment of the event parameters: event cause, coupling factor, detection method, corrective action, CCF root cause and multi-unit event severity. The following noteworthy observations can be made.

- Multi-unit events were observed for a wide range of component types. Emergency diesel generators and centrifugal pumps accounted for more than 50% of the events.
- The most common CCF root cause for multi-unit CCF events is deficiency in the design of components and systems, while nearly 60% of the events had design as the sole or predominant CCF root cause. Events with design as the predominant CCF root cause and environment as a contribution cause are significantly overrepresented. Events with procedures or human action as the predominant CCF root cause and the environment as contributing cause are not overrepresented. This indicates that multi-unit events that involve environmental effects usually require design improvements to prevent reoccurrence. Events with observed environmental deficiencies were caused by harsh environmental conditions, such as severe weather or abnormal debris in a raw water source.
- About 10% of the events were complete multi-unit CCF events, meaning that all the impacted components at all the impacted units were completely failed. This is the most severe type of CCF event.

The analysis of engineering aspects resulted in several important findings. Correlation factors between events were identified, i.e. the multi-unit event dependency. Some multi-

unit events were identified as candidates for the multi-unit site probabilistic safety assessment (MUPSA) modelling. In addition, actual defences that prevented all components from failing and possible defences and improvements to prevent the events from happening again are presented.

A number of conclusions can be drawn from the analysis of multi-unit events. The engineering aspects of the multi-unit events, divided by internal/external correlation factors, are:

Insights on the internal factors

- A total of 57 events were dependent on internal factors, with 27 of these events correlated by "identical design" and 17 correlated by "organisational aspects".
- There were no events in the database where an external factor affected multiple sites; since there are severe events of that type in the operating history of nuclear power plants (e.g. Fukushima Daiichi) it can be concluded that it is very difficult to develop a complete collection of such events.
- The most common correlation factor was "identical design". Events were correlated through the same design of components/systems, operating environment, and installation. Also, some events were correlated as a result of the use of the same unsuitable grease/lubrication. The correlation factor "human" involves issues with maintenance actions such as cleaning (grease) or improper fixing. The correlation factor "organisational aspects" concerns mainly incorrect procedures (both test and maintenance).
- Several interesting CCF events were highlighted during the event analysis with the goal of identifying defences against CCFs. All of these interesting CCF events had internal correlation factors. The interesting CCF events included:
  - those detected outside of normal periodic and planned testing and inspections (11 events identified);
  - those revealing that a set of components was not capable of performing its safety function over a long period of time (five events identified);
  - those where several lines of defence had failed (two events identified);
  - those that originated from deficiencies in safety culture management (five events identified).
- Five of the nine complete CCF events had an internal correlation factor. Three of the five events were correlated by "identical design" and two by "organisation". Several types of improvements were suggested, such as improved design and revising procedures.
- The identified actual defences against events developing into complete CCFs include adequate test and maintenance procedures and inspections. Also, some failures had developed slowly over time and were detected before developing into complete CCFs.
- Feasible defence strategies are proposed to prevent failures from developing into complete CCFs. Feasible defence strategies include well-functioning testing procedures, maintenance procedures, operating experience feedback and the use of skilled personnel. Adequate and robust system/component design is the

fundamental defence against complete CCFs. If the event severity is considered, it can be concluded that for most of the events, adequate defences exist, but for 15 events no actual defence could be identified.

- The most common improvement areas were design of component, surveillance of component or maintenance procedure for component, testing procedure and management system of plant.
  - *Design of component:* Most of the improvements only concerned improvements of the component design.
  - *Testing procedure:* Was common among the internal factor events. The improvements concerned testing requirements, post-testing (often after a modification) and improved test procedures. It is therefore important to have well-functioning procedures to be able to detect the events in time before developing into complete failures.
  - *Surveillance/maintenance:* Only a few events were related to improvements of inspections and the surveillance of component groups. For the events in this area, updates of procedures, quality assurance (QA) of maintenance, and some specific maintenance actions were suggested.
  - *Management system of plant:* Concerned mainly improvements of different QA parts of the management system of plant.

Insights on the external factors

- A total of 14 events were dependent on external factors, with ten of these events correlated to "shared structures, systems and components (SSCs)".
- About 43% of the external factor events were detected at both/with all units at the site at full power.
- Interesting CCF events marked as "multiple systems affected" and "common-cause initiator" involved (not exclusively) external correlation factors.
- While only 16% of all multi-unit events were related to external factors, four of the nine complete CCFs had an external correlation factor, more specifically "shared SSCs". As defence, a better design of the water intake (such as adding back-flushing capability or cleaning the strainers) was suggested for three events and improved maintenance procedure for the fourth event.
- Actual defences were difficult to identify for the non-complete CCF events. However, for some events, surveillance during maintenance and local checks revealed the problems in time. For another event, the failure had been developing slowly over time and was detected during maintenance activity before all components failed.
- Improvements to the *design of system or site* involved both internal and external factor events, but this area was suggested for about half of the events with an external correlation factor. Improvements in *surveillance/maintenance* were also common.
- The external factor multi-unit events have some overlap with a prior ICDE report on CCFs due to external factors (NEA, 2015). This prior report focused on single unit external factors.

Insights on the fleet CCF events

A total of 16 fleet events were identified and about 67% of the events occurred within one year. The number of sites affected ranged from two to five. All the identified fleet CCF events were correlated by internal factors. However, these types of events were excluded in the second data analysis workshop to focus the analysis on single site events.

MUPSA modelling

It is expected that if the single unit PSA is extended to a MUPSA, the physical connections and dependencies across unit boundaries will be accounted for and explicitly modelled. Thus, the 14 external factor events would be useful in identifying important cross-unit dependencies. In addition, for the 57 internal factor events, new CCF groups may need to be defined to combine common-cause component groups across units at the site.

References

1. 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.
2. NEA (2015), "ICDE Workshop on Collection and Analysis of Common-Cause Failures due to External Factors", NEA/CSNI/R(2015)17, OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_19670.

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 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, preparation for the International Common-cause Data Exchange (ICDE) Project began 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 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 the United States (NRC).

More information about the ICDE project can be found on the NEA website: 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 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 a Microsoft access 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 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 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 Database 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;
- incipient failure of the component;

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

- default: component is working according to specification.

Complete CCF events are of particular interest. A "complete CCF event" is defined as a dependent failure of all components of an exposed population where the fault state of each of its components is "complete failure to perform its function" and where these fault states exist simultaneously and are the direct result of a shared cause. Thus, 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 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 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 (ECs), the corrective actions (CAs) and the coupling factor (CF) insights regarding the CCF root causes[6] of the multi-unit 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 corrective action.

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 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 at all (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) 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

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.

Annex 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.

Annex 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

Annex Table 1.D.3. Second root cause aspect – event cause (continued)

	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)**
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.

Annex Table 1.D.4. 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 pre-analysis of the events included in the workshop identifies:

- If the events are multi-unit events (occurred within one year) or recurring events (more than one year in between the events).
- If the events affected several units at one site and/or multiple units at multiple sites:
  - ***Site event:*** The events have affected several units at one site.
  - ***Fleet event:*** The events have affected several units at several sites. (Screened out in the second WS).
- The multi-unit event impairment vector (sum of the individual ICDE event impairment vectors) for question three below.

Questions to be answered:

1. Topical question: Do you agree with pre-analysis of the events? If not, explain why.
2. Topical question: Which factors connect the multi-unit events? (See Table 1.E.1.)
3. Topical question: Specify the ICDE *event impairment vectors* in the multi-unit event.
4. 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.* Provide the answer in the analyst comment field.
5. Specify the plant state (in operation, revision, etc.) when the events were detected. *Note: the plant state could be different between the events in the multi-unit event group.*
6. <u>If not complete CCF:</u>
   a. Can you identify any **actual defences** that prevented all components to fail? **Assign** these with the available categories a-f?
   b. Can you identify any **areas of improvement** in order to prevent the event from happening again? **Assign** these with the available categories a-f?
7. <u>If complete CCF:</u> Can you identify any **possible defences or areas of improvement** that could have prevented all components to fail? **Assign** these with the available categories a-f?
8. If the event is of special interest to others mark the event with applicable "event Category(s)".

Available categories for questions 6 and 7:

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.).

To determine the common factor(s) between the events in topical question 2, Table 1.E.1 presents possible correlation factors. The terminology is explained below.

Definition of ***"internal factors with multi-unit effects"***: Multi-unit events sharing a common internal factor, which affects several units. Categories 1-3 are applicable for these events.

Definition of ***"external factors"***: Multi-unit events with a common external factor. Categories 4-5 are applicable, but also categories 1-3 could be applicable.

Available categories for internal/external factors are:

1. *Organisational:* e.g. management system or instruction based factors.

2. *Human:* e.g. operator actions, maintenance actions.

3. *Identical design:* e.g. same design, – operation and – installation.

4. *Proximity:* e.g. area event, external event, site layout. A subcategory of proximity is *initiating events*, e.g. loss of off-site power.

5. *Shared SSCs:* e.g. connected systems, structures and components.

Annex Table 1.E.1. Available correlation factors

Correlation factors				
Internal factors with multi-unit effects			***External factors***	
1. Organisational	***2. Human***	***3. Identical design***	***4. Proximity***	***5. Shared SSCs***
a) Incorrect procedure	*Pre-initiator*	a) Same design	a) Area event	a) Connected systems, structures and components
b) Latent design issue	a) Missing surveillances	b) Same operation	b) External event	b) Cooling
c) Incorrect calculation	b) Maintenance cleaning	c) Operating environment	c) Site layout	c) Ventilation
d) Incorrect technical specifications	c) Identical installations	d) Same installation	d) Conduits and doors (may connect otherwise independent areas)	d) Signals
e) Incorrect vendor guidance	d) Transposition errors	e) Maintained nearly identically		e) Common parts
f) Incorrect engineering judgement	e) Identical maintenance actions			
g) A misinterpretation of guidance or requirements	*Post-initiating*			
h) A misunderstanding of system configuration or function	f) Misalignment of breakers after LOOP or SBO			
i) Poor safety culture, which leads to errors of judgement and execution across the organisation	g) Misalignment of valves after transient			
j) Lack of adequate training and skills	h) Mental slip because of lack of attention to other units after an event			