Nuclear Safety
NEA/CSNI/R(2017)8
August 2017
www.oecd-nea.org

Workshop on the Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Populations

International Common-Cause Failure Data Exchange (ICDE) Project Report

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

For Official Use **NEA/CSNI/R(2017)8**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

24-Aug-2017

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2017)8
For Official Use

Workshop on the Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Populations

International Common-Cause Failure Data Exchange (ICDE) Project Report

JT03418043

Complete document available on OLIS in its original format

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 35 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

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

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

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 31 countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Korea, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission and the International Atomic Energy Agency also take part in the work of the Agency.

The mission of the NEA is:

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

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

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

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

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

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

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

Foreword

Common-cause failure (CCF) events can significantly impact the availability of safety systems of nuclear power plants. For this reason, the International Common-Cause Failure Data Exchange (ICDE) Project was initiated by several countries in 1994. In 1997, the Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) formally approved the carrying out of this project within the NEA framework; since then the project has successfully operated over five consecutive terms (the current term being 2015-2018).

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

The objectives of the ICDE Project are to:

- Collect and analyse 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 which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences.
- Establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defences against their occurrence, such as indicators for risk-based inspections.
- Generate quantitative insights and record event attributes to facilitate 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 actually contributed data to the databank.

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

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

- Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(99)2], September 1999.

- Collection and analysis of common-cause failure of emergency diesel generators [NEA/CSNI/R(2000)20], May 2000.
- Collection and analysis of common-cause failure of motor-operated valves [NEA/CSNI/R(2001)10], February 2001.
- Collection and analysis of common-cause failure of safety valves and relief valves [NEA/CSNI/R(2002)19]. Published October 2002.
- Collection and analysis of common-cause failure of check valves [NEA/CSNI/R(2003)15], February 2003.
- Collection and analysis of common-cause failure of batteries [NEA/CSNI/R(2003)19], September 2003.
- ICDE General Coding Guidelines [NEA/CSNI/R(2004)4], January 2004.
- Proceedings of ICDE Workshop on the qualitative and quantitative use of ICDE Data [NEA/CSNI/R(2001)8, November 2002.
- Collection and analysis of common-cause failure of switching devices and circuit breakers [NEA/CSNI/R(2008)01], October 2007.
- Collection and analysis of common-cause failure of level measurement components [NEA/CSNI/R(2008)8, July 2008.
- Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(2013)2], June 2013.
- Collection and analysis of common-cause failure of control rod drive assemblies [NEA/CSNI/R(2013)4], June 2013.
- Collection and analysis of common-cause failure of heat exchangers, [NEA/CSNI/R(2013)2], June 2013.
- Collection and Analysis of Common-Cause Failures of Heat Exchangers [NEA/CSNI/R(2015)11], April 2013
- ICDE Workshop on Collection and Analysis of Common-Cause Failures due to External Factors, [NEA/CSNI/R(2015)17], October 2015.

Acknowledgements

The following individuals have significantly contributed to the preparation of this report by their personal effort: Albert Kreuser (GRS), Jeffery Wood (NRC), Anna Georgiadis (ÅF), Gunnar Johanson (ÅF), Mattias Håkansson (ÅF) and Wolfgang Werner (SAC).

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. Axel Breest has been the administrative NEA officer and contributed to finalising the report.

Table of content

List of figures:

List of tables:

List of abbreviations and acronyms

AC	Alternating current
BWR	Boiling water reactor
CCF	Common-cause failure
DC	Direct current
DiD	Defence in depth
DG	Diesel generator
EDG	Emergency diesel generator
ESW	Essential service water
FC	Failure to stop
FR	Failure to run
FS	Failure to start
HVAC	Heating, venting and air conditioning
I&C	Instrumentation and controls
ICDE	International Common-Cause Failure Data Exchange
LER	Licensing event report
LM	Level measurement
LLS	turbine driven emergency power supply
LOCA	Loss of coolant accident
LOOP	Loss of off-site power
NPP	Nuclear power plant
OA	Operating agent
OP	Observed population
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
PWR	Pressurised water reactor
RPS	Reactor protection system
QA	Quality assurance
SAC	Scientific Advisory Committee
SOP	Station operation procedure

ORGANISATIONS

AECB	Atomic Energy Control Board (Canada)
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee on the Safety of Nuclear Installations (NEA)
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat/ Swiss Federal Nuclear Safety Inspectorate (Switzerland)
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (France)
KAERI	Korea Atomic Energy Research Institute (Korea)
NEA	Nuclear Energy Agency
NRA	Nuclear Regulation Authority (Japan)
NRC	Nuclear Regulatory Commission (USA)
OECD	Organisation for Economic Co-operation and Development
ONR	Office for Nuclear Regulation (United Kingdom)
SSM	Swedish Radiation Safety Authority (Sweden)
STUK	Finnish Centre for Radiation and Nuclear Safety (Finland)
UJV	UJV Rez a.s. (Czech Republic)

Executive summary

This report documents a study performed on a set of common-cause failure (CCF) events for diesel generators. The events were derived from the International CCF Data Exchange (ICDE) database and the study was focused on identifying failure mechanisms that are able to affect all diesels in an exposed population in any way, i.e. all events in the ICDE diesel database with no component coded "working" in the exposed population were analysed. The study is based on a workshop performed during an ICDE Steering Group meeting in May 2013 and a number of additional workshops which were performed by the operating agent (OA). In total, 142 ICDE events have been assessed.

This report begins with an overview of the entire data set (Section 3). Charts and tables are provided exhibiting the event count for each of the event parameters such as failure modes, root causes, coupling factors, detection methods and corrective actions. In addition, the events are distributed according to their degree of severity. Generally it could be seen that the most common severity degrees are the least severe, "CCF impaired" and "Complete impairment", which indicates the need to not only focus failure analyses on events where all exposed components have failed completely. A typical diesel event is an event with hardware related failure cause which is detected during maintenance/test and corrected by design modifications.

Engineering insights about the collected events are presented (section 4). The result includes several suggested areas of improvements and prevention from reoccurrence. As an introduction to this section, an overview of concluded failure mechanisms for a number of the events are presented in tables. The failure mechanism describes the observed event and influences leading to a given failure. Elements of the failure mechanism could be a deviation or degradation or a chain of consequences. It is derived from the event description and should preferably consist of one sentence.

There were six categories of improvements to choose from during the workshops and for context purposes, examples of typical events are presented along with each category. The most common assigned category was "Maintenance or testing of component" (34%). Many of these events involve improper re-installations or re-assemblies after testing/maintenance. For example, in one event the governors were incorrectly replaced after testing/maintenance. Suitable prevention for this kind of failure is improved test/maintenance procedures which includes checks after finished test/maintenance.

Regarding preventions from reoccurrence, improved maintenance procedures was identified as a suitable measure in order to prevent all components to fail. Approximately 15% of the events were concluded with this type of prevention. However, the most common answer (23%) to the question "what has or could have prevented all components to fail" was that the failure was slowly developing over time and was therefore detected before all components failed. Another noteworthy comment is that only one event was concluded as "Nothing happened because the problem was detected by failure in other unit at the same site". This indicates the importance of informing other units and plants when an event has occurred, as a preventive action.

In summary, it can be stated that a significant number of CCF events for diesel generators which affected all redundant components simultaneously have been found. In many cases improper maintenance activities caused the failures, so the strict implementation and use of suitable maintenance procedures would have prevented many of the observed events.

1. Introduction

In accordance with the objective of the ICDE project to generate qualitative insights regarding the root causes of CCF events which can be used to derive approaches for their prevention, a workshop on CCF events of diesels was performed during the ICDE Steering Group meeting in May 2013. The event analysis was not finished during the workshop due to a lack of time. During the upcoming summer the remaining event analyses were performed by the operating agent (OA) for the events that were not covered by the Steering Group's workshop. This report summarises the workshop results and presents an overview of the exchange of CCF data among several countries of diesel failures impacting entire exposed populations, so called "all affected" diesel failures. "All affected" diesel failures involves events where all diesels in an exposed population either failed or were degraded or showed an incipient impairment due the same cause, i.e. no "W" in the impairment vector[1]. The objectives of this report are:

- To describe the data profile of the "all affected" emergency diesel generator ICDE events;
- To develop qualitative insights in the nature of the reported events, expressed by root causes, coupling factors, and corrective actions; and
- To develop the failure mechanisms and phenomena involved in the events, their relationship to the root causes, and possibilities for improvement.

Section 2 presents a description of the diesel event data "all affected". An overview of the contents of the diesel database and summary statistics are presented in Section 3. Section 4 contains some high level engineering insights about the diesel CCF events. These insights are based on failure causes and failure mechanisms. Section 5 provides a summary and conclusions. References are found in Section 6.

The ICDE Project was organised to exchange CCF data among countries. A brief description of the project, its objectives and the participating countries, is given in Appendix A. Appendix B presents the definition of common-cause failures and the ICDE event definitions.

1. The impairment vector presents the impairment status of each component of the Exposed population. C = Complete failure of the component to perform its function, D = Degraded ability of the component to perform its function, I = Incipient failure of the component and W = Component is working. See also Appendix B.

2. Event data description

2.1 Preparation of diesel event data "all affected"

The scope of the workshop was defined by the Steering Group. The group was interested in identifying failure mechanisms that are able to impact all diesels in an exposed population. The group selected events in the ICDE diesel database with no "W" in the impairment vector[1]. Consequently, events where not all exposed components have failed completely were included in the scope which aimed to get broader insights in failure mechanisms that are potentially able to lead to complete common-cause failures of emergency diesel generators. An additional selection criterion was time factor and shared-cause factor "High", which implies that multiple component impairment was discovered within a short time interval and the analyst was confident that multiple impairments were due to the same cause.

The above definitions resulted in a workshop scope of 142 events. An overview of the diesel database and the workshop scope are illustrated in Table 1.

Table 1: Preparation of diesel event data "all affected"

Severity category	Description	No. of diesel events in database May 2013	No. of diesel events – All affected (no "W")	No. of diesel events – All affected AND Time factor AND Shared-cause Factor "High"
(a) Complete CCF	All "C"	38	38	26
(b) Partial CCF	At least two "C" but not complete CCF	24	11	9
(c) CCF impaired	At least one "C" but not partial or complete CCF	73	54	51
(d) Complete impairment	All "D" or "I"	60	60	56
(e) Incipient impairment	Multiple impairments but at least one "W"	23	0	0
In total		**218**	**163**	**142**

1 The impairment vector presents the impairment status of each component of the Exposed population. C = Complete failure of the component to perform its function, D = Degraded ability of the component to perform its function, I = Incipient failure of the component and W = Component is working. See also Appendix B.

3. Overview of database content

3.1 Overview

The workshop scope of 142 events was distributed to eleven work groups. The aim was to let member countries analyse their own events as far as possible. Due to lack of time during the Steering Group's workshop, in total 43 out of 142 events were completely analysed by the OA afterwards.

3.2 Failure modes

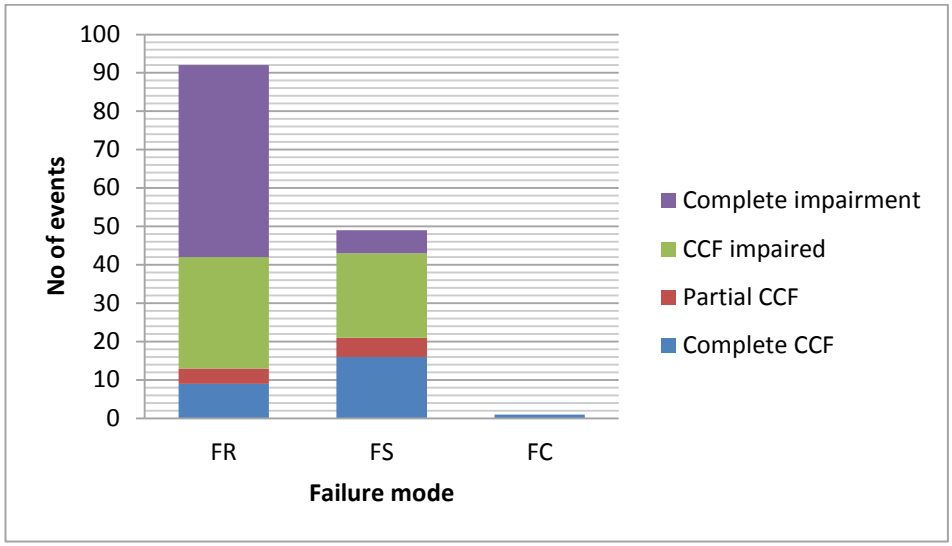
Table 2 and Figure 1 show the distribution of the events by failure mode and severity degree. The most dominant severity degrees are the least severe, "CCF impaired" (c) and "Complete impairment" (d), which indicates the need of not only focusing failure analyses on events where all exposed components have failed completely. About 18% of the analysed events showed a complete failure of all emergency diesel generators in the exposed population.

Table 2: Distribution of severity per failure modes

Failure mode	Number of events	Severity category[1]			
		a	b	c	d
Failure to run (FR)	92	9	4	29	50
Failure to start (FS)	49	16	5	22	6
Failure to stop (FC)	1	1			
Total	**142**	**26**	**9**	**51**	**56**

1. *a) Complete CCF* = All components in the Group are completely failed (i.e. all elements in impairment vector are C, Time factor high and shared-cause factor high.)
   b) Partial CCF = At least two components in the Group are completely failed (i.e. at least two C in the impairment vector, but not complete CCF. Time factor high and shared cause factor high.)
   c) CCF impaired = At least one component in the group is completely failed and others affected (i.e. at least one C and at least one I or one D in the impairment vector, but not partial CCF or complete CCF)
   d) Complete impairment = All components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components. (all D or I in the impairment vector).

Figure 1: Distribution of severity per failure modes



3.3 Root causes

The ICDE general coding guidelines [1] define root cause as follows. The cause field identifies the most basic reason for the component's failure. Most failure reports address an immediate cause and an underlying cause. 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.

Table 3 and

Figure 2 show the distribution of the events by root causes. The dominant root cause for these diesel events is "Design, manufacture or construction inadequacy" (D) which accounts for 38% of the failure events. Many of the events with design related root causes involve construction inadequacy in piece parts, for example parts related to the cooling system and electrical parts. Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel causing insufficient cooling is one example. Another example is wiring errors which led to a too high increase of the diesels' voltage levels.

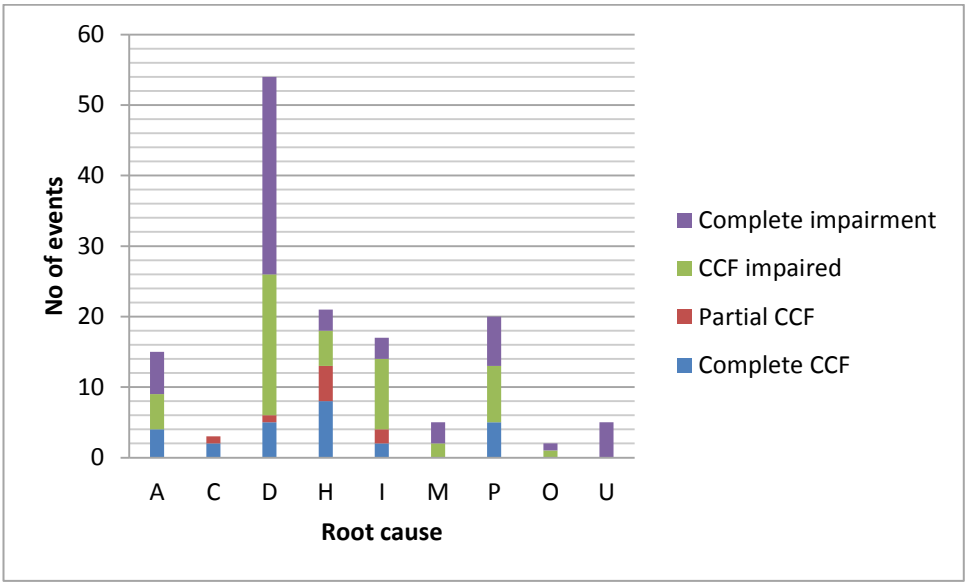
If looking at the distribution of severity it can be seen that complete CCFs represent a relatively large share of the events related to root cause A, H, P (compare with D).

Table 3: Distribution of diesel events "all affected" root causes

Code	Description	No. of Events	Percent	Severity category[2]			
				a	b	c	d
A	Abnormal environmental stress	15	10.6%	4		5	6
C	State of other component(s)	3	2.1%	2	1		
D	Design, manufacture or construction inadequacy	54	38.0%	5	1	20	28
H	Human actions, plant staff	21	14.8%	8	5	5	3
I	Internal to component, piece part	17	12.0%	2	2	10	3
M	Maintenance	5	3.5%			2	3
P	Procedure inadequacy	20	14.1%	5		8	7
O	Other	2	1.4%			1	1
U	Unknown	5	3.5%				5
	Total	**142**	**100.0%**	**26**	**9**	**51**	**56**

2 *a) Complete CCF* = All components in the Group are completely failed (i.e. all elements in impairment vector are C, Time factor high and shared cause factor high.)
b) Partial CCF = At least two components in the Group are completely failed (i.e. at least two C in the impairment vector, but not complete CCF. Time factor high and shared-cause factor high.)
c) CCF Impaired = At least one component in the group is completely failed and others affected (i.e. at least one C and at least one I or one D in the impairment vector, but not partial CCF or complete CCF)
d) Complete impairment = All components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components. (all D or I in the impairment vector).

Figure 2: Distribution of diesel events "all affected" root causes



3.4 Coupling factors

The ICDE general coding guidelines [1] 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 root 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.

These codes are grouped into the following coupling factor category groups:

- Environmental: E, EE, EI;
- Hardware: H, HC, HS, HQ;
- Operations: O, OMF, OMP, OP, OF, OMS.

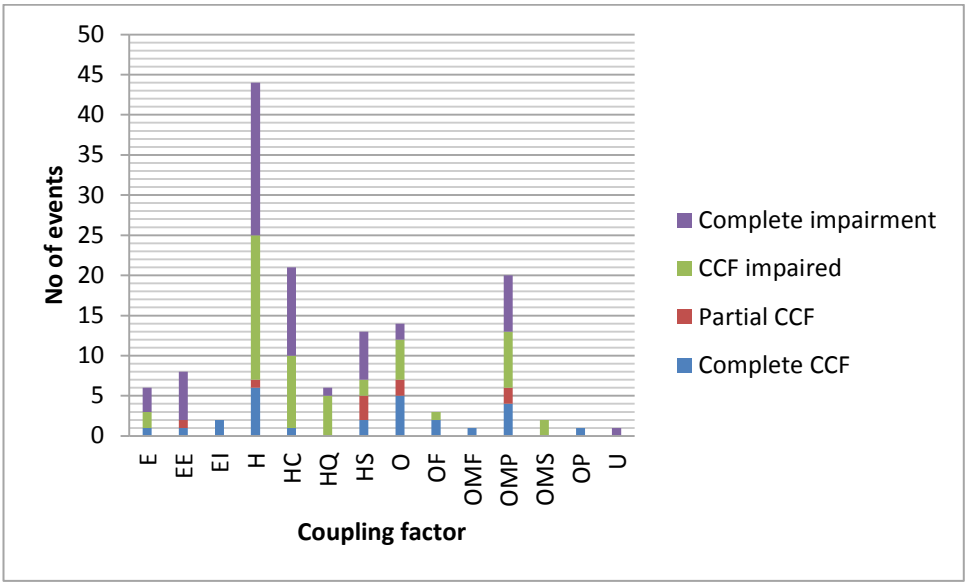
Table 4 and Figure 3 show the distribution of the events by coupling factor. The dominant coupling factor category group is hardware, which accounts for 59% of the diesel events. Many of the events with hardware design coupling factors involve hardware errors in the three-way valves (which control the cooling system of the diesel) which, due to common design (three-way valve within same series), affect several components and cause multiple failures.

Table 4: Distribution of diesel events "all affected" coupling factors

Code	Description	Number of events	Percent	Severity category[3]			
				a	b	c	d
Environment		**16**	**11.3%**	**4**	**1**	**2**	**9**
E	Environment (internal, external)	6	4.2%	1		2	3
EE	Environment External	8	5.6%	1	1		6
EI	Environment Internal	2	1.4%	2			
Hardware		**84**	**59.2%**	**9**	**4**	**34**	**37**
H	Hardware (component part, system configuration, manufacturing quality, installation/configuration quality)	44	31.0%	6	1	18	19
HC	Hardware Design	21	14.8%	1		9	11
HQ	Hardware quality deficiency	6	4.2%			5	1
HS	System Design	13	9.2%	2	3	2	6
Operations		**41**	**28.9%**	**13**	**4**	**15**	**9**
O	Operational (maintenance/test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)	14	9.9%	5	2	5	2
OF	Operation staff	3	2.1%	2		1	
OMF	Maintenance/test Staff	1	0.7%	1			
OMP	Maintenance/test Procedure	20	14.1%	4	2	7	7
OMS	Maintenance/test Schedule	2	1.4%			2	
OP	Operation procedure	1	0.7%	1			
Unknown		**1**	**0.7%**				**1**
Total		**142**	**100.0%**	**26**	**9**	**51**	**56**

3. *a) Complete CCF* = All components in the Group are completely failed (i.e. all elements in impairment vector are C, Time factor high and shared-cause factor high.)
b) Partial CCF = At least two components in the Group are completely failed (i.e. at least two C in the impairment vector, but not complete CCF. Time factor high and shared-cause factor high.)
c) CCF Impaired = At least one component in the group is completely failed and others affected (i.e. at least one C and at least one I or one D in the impairment vector, but not partial CCF or complete CCF)
d) Complete impairment = All components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components. (all D or I in the impairment vector).

Figure 3: Distribution of diesel events "all affected" coupling factors



3.5 Detection method

The ICDE general coding guidelines [1] suggest the following coding for the detection method for each failed component of the exposed population:

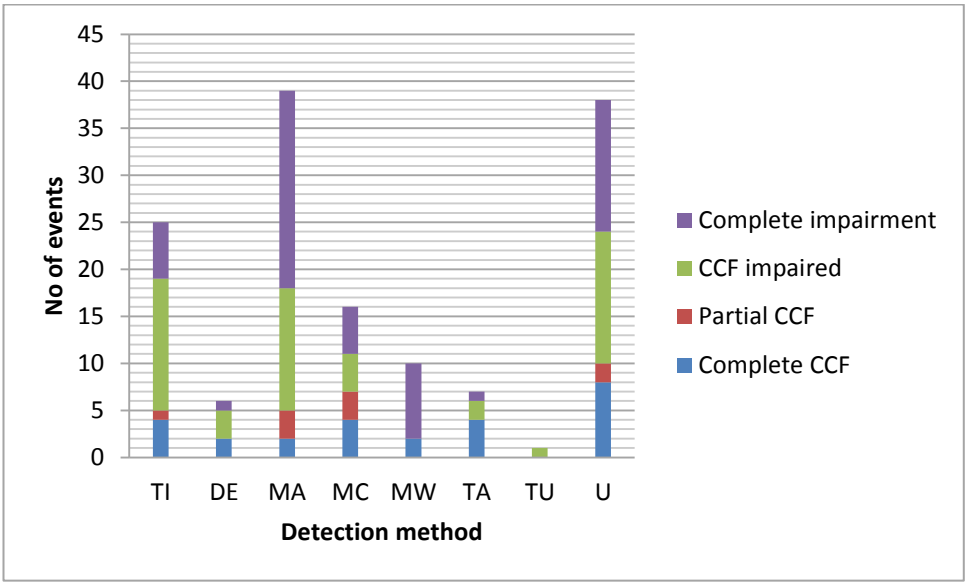
MW	monitoring on walk down
MC	monitoring in control room
MA	maintenance/test
DE	demand event (failure when the response of the component(s) is required)
TI	test during operation
TA	test during annual overhaul
TL	test during laboratory
TU	unscheduled test
U	unknown

Table 5 and Figure 4 contain the distribution of the events by detection method. Maintenance/test was the main way of detecting problems with the diesels, followed by unknown detection methods. The low number of demand events suggests that diesel failures may be easier to detect in periodic tests compared to other type of failures or failures in other components.

Table 5: Distribution of diesel events "all affected" detection modes

Code	Description	No. of Events	Percent	Severity category[4]			
				a	b	c	d
TI	Test during operation	25	17.6%	4	1	14	6
DE	Demand	6	4.2%	2		3	1
MA	Maintenance/Test	39	27.5%	2	3	13	21
MC	Monitoring in Control Room	16	11.3%	4	3	4	5
MW	Monitoring on Walkdown	10	7.0%	2			8
TA	Test during annual overhaul	7	4.9%	4		2	1
TU	Unscheduled test	1	0.7%			1	
U	Unknown	38	26.8%	8	2	14	14
	Total	**142**	**100%**	**26**	**9**	**51**	**56**

Figure 4: Distribution of diesel events "all affected" detection modes



4. *a) Complete CCF* = All components in the Group are completely failed (i.e. all elements in impairment vector are C, Time factor high and shared-cause factor high.)
b) Partial CCF = At least two components in the Group are completely failed (i.e. at least two C in the impairment vector, but not complete CCF. Time factor high and shared-cause factor high.)
c) CCF Impaired = At least one component in the group is completely failed and others affected (i.e. at least one C and at least one I or one D in the impairment vector, but not partial CCF or complete CCF)
d) Complete impairment = All components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components. (all D or I in the impairment vector).

3.6 Corrective actions

The ICDE general coding guidelines [1] define corrective action as follows. The corrective actions field describes the actions taken by the licensee to prevent the CCF event from reoccurring. The defence mechanism selection is based on an assessment of the root 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

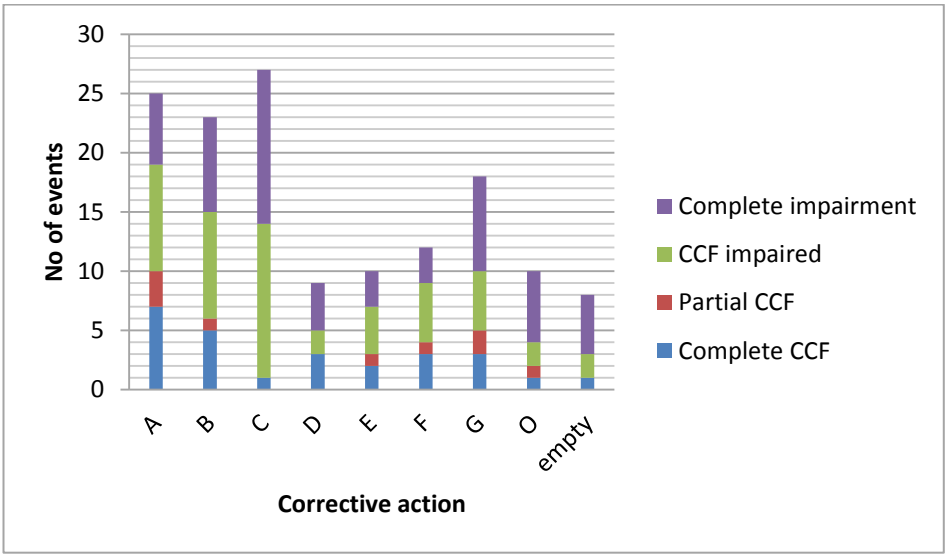
O Other. The corrective action is not included in the classification scheme.

The distribution of the events for corrective actions is shown in Table 6 and Figure 5. 19% of the corrective actions are made by “Design modifications” (C), followed by “General administrative/procedure controls” (A) and “Specific maintenance/operations practices” (A).

Table 6: Distribution of diesel events "all affected" corrective actions

Code	Description	Number	Percent	Severity category[5]			
				a	b	c	d
A	General administrative/procedure controls	25	17.6%	7	3	9	6
B	Specific maintenance/operation practices	23	16.2%	5	1	9	8
C	Design modifications	27	19.0%	1		13	13
D	Diversity	9	6.3%	3		2	4
E	Functional/spatial separation	10	7.0%	2	1	4	3
F	Test and maintenance policies	12	8.5%	3	1	5	3
G	Fixing of component	18	12.7%	3	2	5	8
O	Other	10	7.0%	1	1	2	6
	Empty	8	5.6%	1		2	5
	Total	**142**	**100.0%**	**26**	**9**	**51**	**56**

Figure 5: Distribution of diesel events "all affected" corrective actions



5. *a) Complete CCF* = All components in the Group are completely failed (i.e. all elements in impairment vector are C, Time factor high and shared-cause factor high.)
b) Partial CCF = At least two components in the Group are completely failed (i.e. at least two C in the impairment vector, but not complete CCF. Time factor high and shared-cause factor high.)
c) CCF Impaired = At least one component in the group is completely failed and others affected (i.e. at least one C and at least one I or one D in the impairment vector, but not partial CCF or complete CCF)
d) Complete impairment = All components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components. (all D or I in the impairment vector).

4. Engineering aspects of the collected events

This section contains an engineering review of the diesel events "all affected".

The analysis was based on questions listed in the workshop form, see Appendix C. The questions in the form were aimed to be easy to understand. The participants were also asked to mark interesting events according to the suggested codes, see Appendix D. This marking procedure was a new concept in the project and was introduced and tried for the second time during the workshop.

It was not possible to perform engineering analyses for two events due to sparse information in the event description. Also the analysis for one event was not completed due to that this event was classified as a non-valid CCF event by the utility after it had been reported.

4.1 Plant state

The distribution of the plant state is presented in Table 7. The plant state was not possible to specify for as many as 43 % of the events. However, information about the plant state is not considered essential in this engineering review.

Table 7: Distribution of plant state

Plant state	No. of events	Percent
In operation (100%)	33	23.2%
In revision (0%)	48	33.8%
Unknown	61	43.0%
Total	**142**	**100.0%**

4.2 Marking of interesting events

Marking of interesting events in the ICDE database consists of identifying interesting and extra ordinary CCF event by specific codes and descriptions, for example events where components in more than one group of components or more than one plant were affected by the same failure mechanism (see Appendix D). The identification of important dependency events can provide useful information for the overall operating experience and can also be used as input to pre-defined processes at the utilities. One event can be applied to several codes.

For many of the diesel events it was possible to apply the marking codes according to Appendix D, 10 out of the 12 codes were applied, see Table 8. 110 events were assigned to one mark, 16 events were assigned to 2-3 marks and 16 events were not assigned to any marks at all. In Table 8 it could be seen that the most popular codes, were "CCF Multiple units" and "CCF Complete" (except "No mark applicable").

One of the six events which were assigned three marking codes included an operator which followed the written test procedure and locked the automatic start-up of both diesels, which was in violation of the Technical Specification requirements. What is even more noticeable is that the same event occurred one year before in another unit at the same site where an update process of the test procedure started, but was still ongoing when the same event happened again. Identified prevention

measures are improved communication and quicker update processes and the event was marked with "complete CCF", "Safety culture" and "Multiple units".

Examples of interesting events for each marking code are presented in Table 9 (Section 4.3).

Table 8: Applied interesting event codes

Interesting CCF event code	Description	No. of events	Percent
1 – CCF Complete	Complete failure of all components	27	18.1%
2 – CCF Outside planned test	The event was detected outside of normal periodic and planned testing and inspections	12	8.1%
3 – CCF Component not-capable	Two or more components were not capable to perform its safety function over a long period of time	9	6.0%
4 – CCF Multiple defences failed	Two or more defence in depth levels were affected	2	1.3%
5 – CCF New failure mechanism	Unattended or not foreseen failure mechanism	11	7.4%
6 – CCF Sequence of different CCF	Sequence of different CCF failures and/or subtle dependencies	0	0.0%
7 – CCF Causes modification	Event causes major modification, e.g. exchange of diesel	8	5.4%
8 – CCF Intersystem dependency	Event affecting two or more different systems or functions	0	0.0%
9 – CCF IE_CCI	Event which is both a CCF event and a initiating event causing loss of needed safety system	1	0.7%
10 – Safety culture	Reason of event originates from major deficiencies in safety culture management	8	5.4%
11 – CCF Multiple units	Failure mechanism appeared in a fleet of reactors or multiple units at one site	29	19.5%
12 – No mark applicable	Indicates that event has been analysed but none of the above marks is applicable	41	27.5%
Total		**149**	**100.0%**

4.3 Failure mechanism descriptions

It was established that specifying the failure mechanism was a good start in the analysis process. The failure mechanism describes the observed event and influences leading to a given failure. Elements of the failure mechanism could be a deviation or degradation or a chain of consequences. It is derived from the event description and should preferably consist of one sentence (see Appendix E). The concluded failure mechanisms for all 142 events are presented in Appendix F.

The table below present examples of concluded failure mechanisms for each marking code "interesting events" according to Appendix D. For some marking code categories, the mechanisms have been sorted by relevant mechanism groups (derived from the root cause codes) for a better general view. The following mechanisms groups have been identified:

- Human/operational
- Hardware/design
- External

Some failure mechanisms were marked with more than one code, so these failure mechanisms appear more than once in Table 9.

Table 9: Failure mechanism examples per marking code

Failure mechanism examples for "Complete CCFs" (1)	**Mechanism group**
Cracks in numerous relay sockets were induced by vibrations in the EDG rooms resulting failure of diesel load control	Hardware
ESW strainers were deformed allowing fish to plug ESW components	
External corrosion on cooling pipes due to penetration of rain water because of a non-leak-proof EDG building	
Lockout relay of both EDG output breakers were found sticking (not tripping when required)	
Mechanical fatigue causing pin rupture in pumps that provide fuel to diesels	
Short circuits in two diodes in the rectifier bridge caused a protective fuse to blow, which caused the engine of the EDG to speed during a surveillance test	
A repair work at a reactor protection system cubicle caused a spurious signal that started the DGs. DGs stopped when the signal disappeared.	Human
Erroneous test procedure led to the operator to lock the automatic start-up of both EDG, which was not according to Technical Specification requirements.	
Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply (LLS)	
Improper switch position – the inhibit keys for under voltage protection were in place and the sensor channels for both vital buses were bypassed.	
Incorrect installation of the flow control valves due to procedural inadequacies, inattention to detail and inadequate skills.	
Pollution of the air supply due to sandblasting outside the Diesel building	
Failure mechanism examples for "Outside planned test" (2)	**Mechanism group**
Corrosion of fuel pipe supplying all diesel day tanks due to inappropriate pipeline support (design?).	Hardware
Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply lines.	
Modification to 110 V dc system led to incorrect fuses being used on the diesel system leading to failure to run.	
Unusual high oil consumption let to low oil level, stopping the engine	
Water leakage in cylinder head causing water dripping on overspeed guard and disabling the EDGs electrical control components	
Foam fire system activated in an adjacent room, due to welding fumes from elsewhere entering, where the diesel alternator air intakes were located. Foam could have entered the air intake and caused failure of the diesel.	Human
Pump test procedure leading to wrong position of fuel transfer pump valves leading to not being able to fill day tanks	
Failure mechanism examples for "Component not-capable (3)	**Mechanism group**
Defective potentiometer, DG could not load power controlled	Hardware
Diesel room temperature too high leading to possible failure to run for mission time. Room temperature high due to HVAC control deliberately placed in wrong setting by operators due to a design inadequacy.	
Improper design causing bad ventilation causing high temperature leading to failed transistor and failed voltage regulator and failure of DG	
Thermostatic three-way-valve failure due to valve/rod anti-rotation pin failure	
Circuit breaker failure due to early ageing of a contactor due to voltage change from 220 to 230 V (beyond design)	
Improper greasing of fuel oil pump motor bearings rendered pumps inoperable during extremely cold weather conditions	Human
Valve for cooling water not opened again after repair causing high water temperature	

Failure mechanism examples for "Multiple defences failed (4)	**Mechanism group**
Maintenance carried out in unit 3 instead of unit 4 + unit 4 was reconnected without complete requalification test	Human
Failure mechanism examples for "New failure mechanism" (5)	**Mechanism group**
Glycol leak due to thermal and mechanical stresses could have caused fire during the DGs running because of exhaust proximity	Hardware
Loss of lubrication capacity of the fuel injection pump of DG due to the use of inadequate diesel fuel (low sulfur)	
Oil+graphite paste from open sump contaminating the diesel clutch leading to failed diesel	
Switching operation of transformers led to electromagnetic interference causing tripped tachometer and overspeed protection of diesels	
Turbos of diesel generator units were replaced. The new turbo wall insert was misjudged. The design change produced an unanticipated resonance induced vibration resulting in fatigue failure of a compressor impeller blade.	
Overtemperature of diesel due to dirt deposition on heat exchanger due to high iron content of well water. Depending on circumstances, river or well water is used.	External
Unusual weather conditions with very dense snowing and high wind speed in the direction of the walls caused partial blocking of the combustion air filters.	
Failure mechanism examples for "Causes modification" (7)	**Mechanism group**
External corrosion due to rainwater accumulation of the EDG cooling pipes led to leak	External
Unusual weather conditions with very dense snowing and high wind speed in the direction of the walls caused partial blocking of the combustion air filters.	
DG failed to start due to air valve pistons sticking because of inadequate manufacturing tolerances.	Hardware
Misoperation of the digital time sequencer for automatic loading due to inadequate design.	
Incorrectly replaced governors.	Human
Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply (LLS)	
Failure mechanism examples for "IE_CCI" (9)	**Mechanism group**
Loss of cooling caused by ice forming in the service water pump column (environmental conditions).	External
Failure mechanism examples for "Safety culture" (10)	**Mechanism group**
External corrosion due to rainwater accumulation of the EDG cooling pipes led to leak	External
Inaccurate level instrumentation + human error (not responding to alarm) causing too small fuel level margin without knowing	Hardware + human
2 diesels were taken out of service which was against the station operation procedure SOP	Human
Wrongly re-assembled connector during maintenance leading to that 2 phases were reversed causing wrong spark sequences from exciter which was not detected because of incomplete testing after maintenance	
Erroneous test procedure led to the operator to lock the automatic start-up of both EDG, which was not according to Technical Specification requirements.	
Maintenance carried out in unit 3 instead of unit 4 + unit 4 was reconnected without complete requalification test	
Failure mechanism examples for "Multiple units" (11)	**Mechanism group**
A design modification in the turbocharger of EDGs resulted in resonance vibrations during operation and failures of fan blades	Hardware
Anti-rotation pin failure led to gap between the rod/valve assembly. The pin failure could be caused by non-evolving "metallic fold" defect which probably appeared during the "hot forged" manufacturing process.	
Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel	
Corrosion lead to abnormal wear on fuel supply pipes.	

Cracks in numerous relay sockets were induced by vibrations in the EDG rooms which could result in failure of diesel load control	
Speed oscillations due to a failure of one of the dropping resistors in the governor unit. The resistor failed due to simple long term heat fatigue.	
Filters of the lubrication were found clogged due to fibres in fuel which leads to trip the EDG on "low oil pressure" protection	
Improper strainer assembly which lead to stress on welds and damaged strainer basket + cross-connection of strainers -> causing clogging of both HE (cooling water to DGs)	Human
Undetected low level in diesel fuel supply tank due to undetected miscalibration of LMs after exchange of single LM equipment.	
Sandblast cleaning of the combustion air intercoolers caused sand to be introduced into the engines and then scoring of cylinder liners and piston rings	
External corrosion on cooling pipes due to penetration of rain water because of a non-leak-proof EDG building	External
Failure mechanism examples for "No mark applicable" (12)	
Rain water penetration to the EDG building led to external corrosion, which caused slight leaks on cooling pipes.	External
Improper design of supporting clamps causing vibration and abnormal wear of fuel supply pipes	Hardware
Increase of the voltage of emergency diesel generator outside Tech Spec limits due to inadequate wiring of 140 relays	Human
O-ring of valve piston had aged and hardened, which lead to the failure of both redundant starter valves providing compressed air to the compressors	
Loose anode due to corrosion causing dissonance in cooler	
Leakage of antifreeze from diesel preheating system lead to green sludge in mechanical seal and degraded function of diesel	
Inadequate test procedure resulted in damage of the air start distributer	
Jammed speed regulator due to little exercise causing tripped diesel	
Lack of preventive maintenance resulting in water intrusion of the lube oil caused air system regulator leak (improper component selection assumed) which lead to inadequate downstream pressure of air start system regulator	
Too much torque on the nuts caused fractured surface on the pin bolts in the start air valve, which led to overstrained pin bolts.	
Wrong calibration of single level measurement led to too small volume of fuel storage tank according to Technical Specifications.	

4.3 Areas of improvement and preventions

Six categories of improvements are defined in Table 10. The events were reviewed to determine where the improvement categories could be applied. Each event could be assigned to multiple improvement categories. It resulted in 135 events with one selected category, 46 events with 2-4 selected categories and seven events with no selected categories at all.

In Table 10 it could be seen that the most common assigned category was "Maintenance or testing of component" (34%). Many of these events involve improper re-installations or re-assemblies after testing/maintenance. For example, in one event the governors were incorrectly replaced after testing/maintenance. Suitable prevention for this kind of failure is improved test/maintenance procedures which includes checks after finished test/maintenance. Approximately 15% of the events were concluded with this type of prevention. Within this improvement category the following additional noteworthy insights have been established:

- When planning maintenance activities and procedures the function of ancillary equipment has to be taken into account

- For events which include clogging of oil filters a preventive action could be to add an "oil filter non-clogging verification" on the periodic test procedure consisting of a pressure drop measurement
- Increased redundancy of the level measurements in the diesel fuel tanks combined with staggered testing can detect LM failures such as miscalibrations

Table 10: Distribution of identified improvement categories

Improvement category	No. of events	Percent
a – Design of system or site	15	8.3%
b – Design of component	51	28.2%
c – Surveillance of component	15	8.3%
d – Maintenance or testing of component	61	33.7%
e – Operation of component	10	5.5%
f – Management system of plant[1]	29	16.0%
Total	**181**	**100.0%**

Also the improvement category "Design of component" was common among the events (28%). Improper design of different piece parts such as cooling pipes, three-way-valves (gap rod/valve) and exhaust damper linkage seems to be the problem for many events.

Among the 29 events (16%) which were assigned "Management system of plant", improved QA of the vendor was pointed out several times. Regarding one event better instructions about screwing torque of lock-nut for the three-way valve from the manufacturer would have prevented the event from happening (the lock-nut was not tightened enough). This implies that "QA of vendor" not only involves quality assurance of the actual product but also that the product information delivered together with the product is sufficient.

Examples of events assigned with category "Design of system or site" are accordingly design errors such as corrosion in cooling pipes due to penetration of rain water because of a non-leak-proof EDG building or inadequate vibration tolerant design leading to cracks in the cooling system. Regarding building designs, it is important to implement state-of-the-art practices to handle possible weather phenomena such as rain water.

Examples of events assigned with category "Surveillance of component" are blockage in heat exchanger tubes (primarily corrosion nodules) and unusual high oil consumption which let to low oil level and stopping of the engine. Monitoring the flow in cooling pipes, the oil consumption and also the diesel fuel supply could be an appropriate improvement for these types of events. However, if increasing the number of monitors and alarms in the control room the risk of overlooking important alarms should be considered.

One example of an event assigned with category "Operation of component" is over temperature of diesel due to dirt deposition on heat exchanger due to high iron content of well water. In the concerned plant it is possible to use river or well water depending on the circumstances, and with regard to this event, operation with river water could have prevented the event from happening. As lesson learnt from this event it can be derived that controlling the water chemistry of the cooling water is important.

The most common answer (23%) to the question "what have or could have prevented all components to fail" was that the failure was slowly developing over time and was therefore detected before all components failed.

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

For one event (welding with in other room activated fire suppression system in the common basement under the diesel rooms where cables are installed) it is concluded that consequent spatial separation of redundancies including ancillary equipment (cables in this case) would have resulted in a less substantial event. Another preventive action for the same event would be to seal possible fume transfer routes (wall penetrations) during maintenance activities.

Another noteworthy comment is that only one event was concluded as "Nothing happened because the problem was detected by failure in other unit at the same site". This indicates the importance of informing other units and plants when an event has occurred, as a preventive action.

25% of the events were left without any answer to this workshop question.

5. Summary and conclusions

The scope of this report includes 142 ICDE diesel events. The aim was to identify failure mechanisms that are able to impact all diesels in an exposed population. The group selected all events in the ICDE diesel database with no "W" in the impairment vector. Consequently, events where not all exposed components have failed completely were included in the scope which aimed to get broader insights in failure mechanisms that are potentially able to lead to complete common-cause failures of emergency diesel generators. An additional selection criterion was time factor and shared-cause factor "High", which implies that multiple component impairment was discovered within a short time interval and the analyst was confident that multiple impairments were due to the same cause. The reported events were reviewed in Sections 3 and 4 with respect to degree of failure, failure causes, failure symptoms and failure mechanism.

The report includes several suggested improvements and other interesting insights. The most common assigned improvement category was "Maintenance or testing of component". Many of these events involve improper re-installations or re-assemblies after testing/maintenance. Suitable prevention for this kind of failures is improved test/maintenance procedures which includes checks after finished test/maintenance.

The most common answer to the question "what have or could have prevented all components to fail" was that the failure was slowly developing over time and was therefore detected before all components failed. This indicates that there is a good chance that the diesel failures are possible to detect "in time".

Marking of interesting events in the ICDE database was a new concept in the project and was introduced and tried for the second time during this workshop. It turned out to be useful and a couple of interesting events were identified and the most popular codes were "CCF Multiple units" and "CCF Complete" (except "No mark applicable").

It was also established that specifying the failure mechanism was a good start in the analysis process. The failure mechanism describes the observed event and influences leading to a given failure. A suggestion of an even more systematic approach to specify the failure mechanism is to divide the failure mechanism in elements, starting with the "trigger" and thereafter "consequence 1", "consequence 2" etc. In this way the failure analysis process is even more transparent and easy to follow and it also facilitates the reporting process. Also the consequences and the identified improvements or defences can be correlated based on this approach.

6. References

NEA (2004), *International Common-Cause Failure Data Exchange ICDE General Coding Guidelines* ICDE CG00, CSNI Tech Note publication NEA/CSNI/R(2004)4. Rev. 2, October 2005.

Appendix A – Overview of the ICDE Project

Appendix A contains information regarding the ICDE project.

A.1 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, the preparation for the international common-cause data exchange (ICDE) project was initiated in August of 1994. Since April 1998 the NEA has formally operated the project, following which the Project was successfully operated over five consecutive terms from 1998 to 2011. The current phase started in 2015 and is due to run until 2018. Member countries under the current Agreement of 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), Spain (CSN), Sweden (SSM), Switzerland (ENSI) and United States (NRC).

More information about the ICDE project can be found at NEA´s web site: www.nea.fr/html/jointproj/icde.html. Additional information can also be found at the web site www.eskonsult.se/ICDE/.

A.2 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, fans, batteries, control rod drive assemblies, circuit breakers, level measurement and digital I&C equipment.

A.3 Data collection status

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

A.4 ICDE coding format and coding guidelines

Data collection guidelines have been developed during the project and are continually revised. They describe the methods and documentation requirements necessary for the development of the ICDE databases and reports. The format for data collection is described in the general coding guidelines and in the component specific guidelines. Component specific guidelines are developed for all analysed component types as the ICDE plans evolve [1].

A.5 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.

Appendix 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, Revision 1 "Common-Cause Failure Data Collection and Analysis System: Event Data Collection, Classification, and Coding:"

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

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

In the context of the data collection part of the ICDE project, focus will be on CCF events with total as well as partial component failures that exist over a relevant time interval1. To aid in this effort the following attributes are chosen for the component fault states, also called impairments or degradations:

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

Complete CCF events are of particular interest. A "complete CCF event" is defined as a dependent failure of all components of an exposed population where the fault state of each of its components is 'complete failure to perform its function' and where these fault states exist simultaneously and are the

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

direct result of a shared cause. Thus, in the ICDE project, we are interested in collecting complete CCF events as well as partial CCF events. The ICDE data analysts may add interesting events that fall outside the ICDE event definition but are examples of recurrent – possibly 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.

Appendix C – Workshop form

1) Specify the plant state (in operation, revision etc.)
2) Describe the failure mechanism[1] including cause of failure in a few words, for example *Vibration due to poor spare parts led to cracks in fuel pipes.*
3) Can any areas of improvement be identified in order to prevent the event from happening again? If so, assign them to the following categories:
   a) Design of system or site
   b) Design of component
   c) Surveillance of component
   d) Maintenance or testing of component
   e) Operation of component
   f) Management system of plant (QA of vendor, spare parts management, training of personnel, sufficient resources/staff etc.)
4) What have or could have prevented all components to fail (if so)? Example: Failure was slowly developing over time and was detected before all components failed.
5) Mark the event with any of the suggested codes in Appendix D. The codes can also be found in the pull down menu in the field “”Event Categories” in Tools.

1. Describes the event and influences leading to a given failure

Appendix D – Codes for marking interesting events

Interesting CCF event codes	Description ***Purpose***
CCF Complete **(1)**	Event has led to a complete CCF. *This code sums up all complete CCFs, for any component type*.
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 DiD level 2.*
CCF Component not-capable **(3)**	Event revealed that a set of components was not capable to perform its safety function over a long period of time. *The code gives information about a deviation from deterministic approaches, when it is revealed that two or more exposed components would not perform the licensed safety function during the mission time.*
CCF Multiple defences failed **(4)**	Several lines of defence failed *More than one line of defence against CCF failed e.g. in the QA processes of designer, manufacturer, TSO and utility during construction and installation of a set of components.*
CCF New failure mechanism **(5)**	Event revealed an unattended or not foreseen failure mechanism. *The code gives information about a new CCF event revealed and a new failure mechanism, not earlier documented in the licensing documentation or operating history.*
CCF Sequence of different CCF **(6)**	Events with a sequence of different CCF failures and /or subtle dependencies *The code gives information about incidents which revealed that more than one CCF failure occurred in different sets of components which were demanded in the event sequence.*
CCF Causes modification **(7)**	Event causes major modification *The code gives information about a CCF event revealed that has led to or will lead to a major plant or system or component modification.*
CCF Intersystem dependency **(8)**	Intersystem dependency. *This indicator gives information about CCFs affecting two or more different systems / functions. The CCF event affects two or more components, functions belonging to several systems. Interesting deviation from deterministic approaches and operating experiences.*
CCF IE_CCI **(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.*
CCF Safety culture **(10)**	The reason to 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.*
CCF Multiple units **(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.*
No mark applicable **(12)**	Indicates that event has been analysed but none of the above marks is applicable.

Appendix E – Suggestion for improving failure analysis approach

During the workshop it was also established that specifying the failure mechanism was a good start in the analysis process. The failure mechanism is describing the observed event and influences leading to a given failure. A suggestion of an even more systematic approach to specify the failure mechanism is presented in the table below. Here the analyst is encouraged to divide the failure mechanism in elements, starting with the "trigger" and thereafter "consequence 1", "consequence 2" etc. In this way the failure analysis process is even more transparent and easy to follow and it also facilitates the reporting process. Also the correlation between the consequences and the identified improvements or defences is illustrated in the same table. For each identified "consequence" in the failure mechanism description the aim is to find a suitable defence. An example, which is based on two different events, illustrates the idea of the new workshop form.

Failure analysis form	Trigger	1st consequence	2nd consequence	3rd consequence
Failure mechanism				
1. Describe the failure mechanism including cause of failure in a few words. The ICDE Observation describes the observed event and influences leading to a given failure.	*Ex 1: Improper assembly of one strainer after maintenance*	*Ex 1: Stress on welds and damaged strainer basket*	*Ex 1: Clogging of both HE which supplies cooling water to the diesels*	
	Ex 2: To stop fuel leak in bulk storage tank, the tank was isolated	*Ex 2: Automatic draining of day tank not possible*	*Ex 2: Excessive fuel contaminated the cam-box lubricating oil of the DGs*	
Improvements/defences				
2. Can any areas of improvement be identified in order to prevent the event from happening again? If so, assign them to the following categories: a) Design of system or site b) Design of component c) Surveillance of component d) Maintenance or testing of component e) Operation of component f) Management system of plant (QA of vendor, spare parts management, training of personnel, sufficient resources/staff etc.) g) What have or could have prevented all components to fail (if so)?	*Ex 1: Include checks after finished maintenance in the maintenance procedure (category d)*	*Ex 1: Often, clogging is a slow process*	*Ex 1: Do not operate the HEs cross-connected (category e)*	
	Ex 2: Increase understanding of the system /component (category f)	*Ex 2: Introduce alternative draining path (category a)*	*Ex 3: Introduce a surveillance routine when automatic function is disconnected (category c)*	

Appendix F – Failure mechanisms for all events

Work event	Concluded failure mechanism
A1	Design error in the diesel governor cooling piping led to too low cooling water flow through the coolers, overheating of governor oil and subsequent governor failure
A2	Due to a design error of the needed power too small EDGs were installed in plant. In case of needing full emergency design loads and not having low ambient temperatures the EDGs would have failed
A3	Cracks in numerous relay sockets were induced by vibrations in the EDG rooms resulting failure of diesel load control
A4	A wiring error in the EDG control panel lead to a too high increase of diesel power when grid voltage gradually increased during a twenty four hours run test
A5	Unit trip relays were reset due to operator error preventing EDGs to pick up load when started
A6	Inadequate test procedure resulted in damage of the air start distributer
A7	Improper greasing of fuel oil pump motor bearings rendered pumps inoperable during extremely cold weather conditions
A8	Use of uncalibrated crimpers resulted in deficient crimp connections in EDG wiring connections and failure to start of a EDG
A9	A design modification in the turbocharger of EDGs resulted in resonance vibrations during operation and failures of fan blades
A10	Cracks in numerous relay sockets were induced by vibrations in the EDG rooms which could result in failure of diesel load control
A11	Installation of 240/480 V AC starting contactor coils in a 125 V DC system resulted in excessive arcing in a control relay making an automatic restart of EDGs impossible
A12	Inadequate manufacturing tolerances resulted in sticking of air valve pistons
A13	Inadequate design of fuel oil transfer valves prevented them to open and to fill up fuel oil in day tanks of EDGs. (Failure to open of valve seems to be connected with thermal pressurisation of a pump discharge piping)
B1	Speed oscillations due to a failure of one of the dropping resistors in the governor unit. The resistor failed due to simple long term heat fatigue
B2	Unusual weather conditions with very dense snowing and high wind speed in the direction of the walls caused partial blocking of the combustion air filters
B3	A repair work at a reactor protection system cubicle caused a spurious signal that started the DGs. DGs stopped when the signal disappeared
B4	Unusual weather conditions with very dense snowing and high wind speed in the direction of the walls caused partial blocking of the combustion air filters
B5	Incorrectly replaced governors
B6	Incorrect installation of the flow control valves due to procedural inadequacies, inattention to detail and inadequate skills
B7	Sandblast cleaning of the combustion air intercoolers caused sand to be introduced into the engines and then scoring of cylinder liners and piston rings
B8	Design deficiency in the carbon dioxide fire protection system auxiliary circuitry caused a fuse to blow
B9	Improper strainer assembly which lead to stress on welds and damaged strainer basket + cross-connection of strainers -> causing clogging of both HE (cooling water to DGs)
B10	Wrong trip settings of safety related circuit breakers + EDG room air temperatures too high due to recirculation of air without tripping of breakers
B11	Improper strainer assembly which lead to stress on welds and damaged strainer basket + cross-connection of strainers -> causing clogging of both HE (cooling water to DGs)
B12	ESW strainers were deformed allowing fish to plug ESW components

Work event	Concluded failure mechanism
B13	ESW strainers were deformed allowing fish to plug ESW components
C1	Increase of the voltage of emergency diesel generator outside Tech Spec limits due to inadequate wiring of 140 relays
C2	Blockage in heat exchanger tubes (primarily corrosion nodules). The nodules originated from failure of an epoxy paint coating
C3	Load failure due to binding of the fuel rack pivot points caused by paint on these components, which occurred during painting of the DGs
C4	Diesel generator not able to reach design load due to misadjusted engine governor output linkage
C5	Loss of lubrication capacity of the fuel injection pump of DG due to the use of inadequate diesel fuel (low sulfur)
C6	The diesel generator did not reach design power level at test due to a defective spare part responsible for the connection of the oil supply with the speed controller
C7	Erratic load control due to intermittent failure of the governor electric control of diesel generator; output breaker opened on a reverse power trip
C8	Turbos of diesel generator units were replaced. The new turbo wall insert was misjudged. The design change produced an unanticipated resonance induced vibration resulting in fatigue failure of a compressor impeller blade
C9	Lockout relay of both EDG output breakers were found sticking (not tripping when required)
C10	Lack of preventive maintenance resulting in water intrusion of the lube oil caused air system regulator leak (improper component selection assumed) which lead to inadequate downstream pressure of air start system regulator
C11	Short circuits in two diodes in the rectifier bridge caused a protective fuse to blow, which caused the engine of the EDG to speed during a surveillance test
C12	O-ring of valve piston had aged and hardened, which lead to the failure of both redundant starter valves providing compressed air to the compressors
C13	Improper switch position – the inhibit keys for under voltage protection were in place and the sensor channels for both vital buses were bypassed,
D1	Misoperation of the digital time sequencer for automatic loading due to inadequate design
D2	Cracks found in the exhaust damper linkage roll pin due to inadequate design
D3	Failed resistor in the governor due to long term heat fatigue
D4	Failure to close of the output breaker led to failure to synchronise the generator to off-site power The switch failed sue to slight breaker movement and/or buildup of oxidation/pitting on the contact surfaces
D5	DG failed to start due to air valve pistons sticking because of inadequate manufacturing tolerances
D6	Lack of ventilation and inadequate cooling in excitation cabinet led to DG failure to continue running
D7	Generator output breaker tripled to failure to synchronise the generator to off-site power
D8	Voltage regulator failure within a certain range of the generator capability (depends by the size of the power potential transformer and the current transformer) causing failure of DG
D9	Description too sparse to complete the failure analysis
D10	Loss of cooling caused by ice forming in the service water pump column (environmental conditions)
D11	Description too sparse to complete the failure analysis
D12	Description too sparse to complete the failure analysis
D13	Cracks in the rubber gland of the engine
E1	Turbocharger damaged due to a piece part that got loose
E2	Exciter switch failure due to an unsuitable spring. The spring had been retrofitted following a recommendation by the manufacturer which was issued after a LER. The spring was unsuitable because the manufacturer had not considered a design change of the switch

Work event	Concluded failure mechanism
E3	Improper design causing bad ventilation causing high temperature leading to failed transistor and failed voltage regulator and failure of DG
E4	Failure due to wrong setpoint of overspeed protection
E5	Poor venting as a result of inclined installation led to low viscosity of oil in oil pressure measurement line and too slow buildup of oil pressure signal, component protection switched diesel off
E6	Vibrations led to the widening of the clearance between limit switch tapped and actuator cam. Diesel was shut off by component protection
E7	Inaccurate level instrumentation + human error (not responding to alarm) causing too small fuel level margin without knowing
E8	Overtemperature of diesel due to dirt deposition on heat exchanger due to high iron content of well water. Depending on circumstances, river or well water is used
E9	Leakage of internal cooling due to corrosion
E10	Circuit breaker failure due to early ageing of a contactor due to voltage change from 220 to 230 V (beyond design)
E11	Re-using of piece part instead of replacement with new led to fuel leakage
E12	Switching operation of transformers led to electromagnetic interference causing tripped tachometer and overspeed protection of diesels
E13	Valve for cooling water not opened again after repair causing high water temperature
F1	Elastic coupling between generator and diesel motor broke. Durability (life time) shorter than specified by supplier
F2	Pump test procedure leading to wrong position of fuel transfer pump valves leading to not being able to fill day tanks
F3	Jammed speed regulator due to little exercise causing tripped diesel
F4	Jammed speed regulator in fuel pump causing insufficient speed in order to start diesels
F5	Loose connection to speed counter leading to no signal that right rpm was achieved, causing error alarm during diesel start-up
F6	Seized fuel pump probably due to too dry oil and inappropriate storage tanks
F7	Wrongly re-assembled connector during maintenance leading to that 2 phases were reversed causing wrong spark sequences from exciter which was not detected because of incomplete testing after maintenance
F8	During maintenance valve and tube are locked with screw causing tube to become oval which lead to air leakage and long start-up time of diesels
F9	Dehydration causing cracks in fuel hose
F10	Too much torque on the nuts caused fractured surface on the pin bolts in the start air valve, which led to overstrained pin bolts
F11	Oblique tightening of the pump house lid led to the plunger in the fuel valve was stuck which led to jamming of the fuel pump cylinder leading to low exhaust temperature
F12	Wrong material of bolts led to fatigue which caused the pin bolts to the start air valve to crack and become loose
F13	Contamination (mostly iron) led to the measure pipe to clog in the internal cooling water system leading to alarm for low water pressure
F14	Wrong calibration of single level measurement led to too small volume of fuel storage tank according to Technical Specifications
G1	Human error which led to blockage of fuel due to valve misalignment
G2	Filters of the lubrication were found clogged due to fibres in fuel which leads to trip the EDG on "low oil pressure" protection
G3	Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply (LLS)

Work event	Concluded failure mechanism
G4	Pollution of the air supply due to sandblasting outside the Diesel building
G5	External corrosion due to rainwater accumulation of the EDG cooling pipes led to leak
G6	Coupling pins failure led of loss of fuel supply preventing the EDG to start
G7	Glycol leak due to thermal and mechanical stresses could have caused fire during the DGs running because of exhaust proximity
G8	Loss of grid + 2 diesels were mistakenly shut down + electrical supply switched back from DG to grid without resetting reactor shutdown system + no training when loss of grid + reactor shutdown causing complete failure of 2 diesels
G9	To stop water leak in fire protection system, valve was opened which led to low air pressure in fire protection system which led to fire protection system becoming unavailable which led to GT3 and GT4 becoming unavailable for seven seconds
G10	Anti-rotation pin failure caused the rod lock-nut to unscrew which led to incorrect stroke of the three-way valve in the engine water cooling system
G11	Anti-rotation pin failure led to gap between the rod/valve assembly. The pin failure could be caused by non-evolving “metallic fold” defect which probably appeared during the “hot forged” manufacturing process
G12	Mechanical fatigue causing pin rupture in pumps that provide fuel to diesels
H1	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply lines
H2	Fibres clogged the lubrication system of EDG
H3	Locking of automatic start-up of both EDGs were erroneously required by the test procedure
H4	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply lines
H5	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply lines
H6	External corrosion on cooling pipes due to penetration of rain water because of a non-leak-proof EDG building
H7	Improper injection pump fixing on the EDG casing. The pump breakage was due to three screws rupture on the injection pump cover caused by vibrations generated during the EDG running
H8	Malfunction of thermostat which controls the cooling system of the diesels
H9	The cause of this incident was due to the three-way valve malfunction
H10	Inadequate design of the three-way valve led to the valve stayed in wrong position, which caused “cooling bypass” and the “max water temperature” protection tripped in the engine water cooling system
H11	Insufficient tightening of the screws of the rod/valve assembly in the three-way valve led to tripping of the “max water temperature” protection in the engine water cooling system
H12	Erroneous test procedure led to the operator to lock the automatic start-up of both EDG, which was not according to Technical Specification requirements
H13	Maintenance carried out in unit 3 instead of unit 4 + unit 4 was reconnected without complete requalification test
I1	Foam fire system activated in an adjacent room, due to welding fumes from elsewhere entering, where the diesel alternator air intakes were located. Foam could have entered the air intake and caused failure of the diesel
I2	Corrosion of fuel pipe supplying all diesel day tanks due to inappropriate pipeline support (design?)
I3	Loss of oil from diesel room cooling fans gearbox causing fan failure. Cause of oil loss was maintenance work inside the diesel room impacting/disturbing the oil pipework
I4	Design of diesel air manifold led to cracking in operation/over time
I5	High resistance of breaker contacts due to hardening of contact lubricant grease. This led to auto-start being inhibited
I6	Following fire testing where the pressure switches are activated manually, the master relay was not reset due to misunderstanding. This would have prevented the diesels connecting and supplying power to the essential electric board
I7	Diesel room temperature too high leading to possible failure to run for mission time. Room temperature high due to HVAC control deliberately placed in wrong setting by operators due to a design inadequacy

Work event	Concluded failure mechanism
I8	Low air pressure prevented start of diesels. Air pressure due to different faults with the two compressors and reliance of all three diesels on the two compressors
I9	Modification to 110 V dc system led to incorrect fuses being used on the diesel system leading to failure to run
I10	2 diesels were taken out of service which was against the station operation procedure SOP
I11	Oil+graphite paste from open sump contaminating the diesel clutch leading to failed diesel
I12	Governor processor failed due to computer failure, which led to alarm and gas turbine GT2 trip. Similar alarm for GT1
I13	Leak in bulk storage tank lead to isolation of tank which lead to automatic draining of day tank not possible. Excessive fuel contaminated the cam-box lubricating oil of the DGs
J1	Control cable cut off by worker, loss of monitoring
J2	Inadequate vibration tolerant design, vibration induced fatigue cracking and inadequate post-modification testing lead to leakage of cooling water jacket
J3	Loose anode due to corrosion causing dissonance in cooler
J4	Unusual high oil consumption let to low oil level, stopping the engine
J5	Defective potentiometer, DG could not load power controlled
J6	Insufficient torqued screw prevented DG to start
J7	Pressure peak caused leakage in cooling
J8	Undetected low level in diesel fuel supply tank due to undetected miscalibration of LMs after exchange of single LM equipment
J9	Water leakage in cylinder head causing water dripping on overspeed guard and disabling the EDGs electrical control components
J10	Water leakage in cylinder head causing water dripping on overspeed guard and disabling the EDGs electrical control components
J11	Spurious trip of relay without any reason caused blocking of automatic diesel start if demanded
J12	Leakage in fuel pipes due to disconnected fitting and faulty orientation of bolts
K1	External corrosion on cooling pipes due to penetration of rain water because of a non-leak-proof EDG building
K2	Cylinder injection pump broke because of screws rupture due to improper pump fixing
K3	Thermostatic three-way-valve failure due to valve/rod anti-rotation pin failure
K4	Corrosion lead to abnormal wear on fuel supply pipes
K5	Corrosion lead to abnormal wear on fuel supply pipes
K6	Improper installation of the rod/drive shaft on the three-way valves lead to loss of cooling, which would have led to unavailability of both EDGs
K7	Leakage of antifreeze from diesel preheating system lead to green sludge in mechanical seal and degraded function of diesel
K8	Improper design of supporting clamps causing vibration and abnormal wear of fuel supply pipes
K9	Malfunction of thermostat which controls the cooling system of the diesels
K10	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel
K11	Rain water penetration to the EDG building led to external corrosion, which caused slight leaks on cooling pipes
K12	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel
K13	The rod lock-nut was unscrewing which led to incorrect stroke of the three-way valve in the engine water cooling system

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.

Complete common-cause failure: A common-cause failure in which all redundant components are failed simultaneously as a direct result of a shared cause (i.e. the component impairment is 'Complete failure' for all components and both the time factor and the shared-cause factor are 'High').

Component: An element of plant hardware designed to provide a particular function.

Component boundary: The component boundary encompasses the set of piece parts that are considered to form the component.

Coupling factor/mechanism: 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.

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

Exposed population (EP): A set of similar or identical components actually having been exposed to the specific common causal mechanism in an actually observed CCF event.

Failure: The component is not capable of performing its specified operation according to a success criterion.

Failure cause: The most readily identifiable reason for the component failure. The failure cause category is specified as part of the failure analysis coding, which provides additional insights related to the failure event.

Failure cause categories: A high level and generalised list of deficiencies in operation and in design, construction and manufacturing which caused an ICDE event to occur.

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

Failure mechanism categories: Are component-type-specific groups of similar Failure mechanism sub-Categories.

Failure mechanism sub-categories: Are coded component-type-specific observed faults or non-conformities which have led to the ICDE event.

Failure mode: The failure mode describes the function the components failed to perform.

Degraded failure: The component is capable of performing the major portion of the safety function, but parts of it are degraded. For example, high bearing temperatures on a pump will not completely disable a pump, but it increases the potential for failing within the duration of its mission.

ICDE event: Impairment 1) of two or more components (with respect to performing a specific function) that exists over a relevant time interval 2) and is the direct result of a shared cause.

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

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

Root cause: The most basic reason for a component failure, which, if corrected, could prevent recurrence. The identified root cause may vary depending on the particular defensive strategy adopted against the failure mechanism.

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

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