Nuclear Safety
NEA/CSNI/R(2018)5
September 2018
www.oecd-nea.org

Lessons Learnt from Common-Cause Failure of Emergency Diesel Generators in Nuclear Power Plants

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

OECD
BETTER POLICIES FOR BETTER LIVES

60th anniversary
NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CSNI/R(2018)5

Unclassified

English text only

26 September 2018

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Lessons Learnt from Common-Cause Failure of Emergency Diesel Generators in Nuclear Power Plants

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

JT03436132

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 36 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, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, 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 33 countries: Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission also takes part in the work of the Agency.

The mission of the NEA is:

– to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally sound and economical use of nuclear energy for peaceful purposes;

– to provide authoritative assessments and to forge common understandings on key issues as input to government decisions on nuclear energy policy and to broader OECD analyses in areas such as energy and the sustainable development of low-carbon economies.

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

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) 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 Committee on the Safety of Nuclear Installations (CSNI) formally approved this project within the NEA framework. Since then, the project has successfully operated over six consecutive terms (the current term being 2015-2018).

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

The objectives of the ICDE Project are to:

1. Collect and analyse common-cause failure (CCF) events over the long term so as to better understand such events, their causes, and their prevention.
2. Generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences.
3. Establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defences against their occurrence, such as indicators for risk-based inspections.
4. Generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries.
5. Use the ICDE data to estimate CCF parameters.

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

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

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

- Collection and analysis of CCF of centrifugal pumps [NEA/CSNI/R(99)2], September 1999.
- Collection and analysis of CCF of emergency diesel generators [NEA/CSNI/R(2000)20], May 2000.
- Collection and analysis of CCF of motor-operated valves [NEA/CSNI/R(2001)10], February 2001.
- Collection and analysis of CCF of safety valves and relief valves [NEA/CSNI/R(2002)19], October 2002.
- Collection and analysis of CCF of check valves [NEA/CSNI/R(2003)15], February 2003.
- Collection and analysis of CCF of batteries [NEA/CSNI/R(2003)19], September 2003.
- Proceedings of ICDE Workshop on the qualitative and quantitative use of ICDE Data [NEA/CSNI/R(2001)8, November 2002.
- Collection and analysis of CCF of switching devices and circuit breakers [NEA/CSNI/R(2008)01], October 2007.
- Collection and analysis of CCF of level measurement components [NEA/CSNI/R(2008)8, July 2008.
- ICDE General Coding Guidelines – Updated Version [NEA/CSNI/R(2011)12], October 2011.
- Collection and analysis of CCF of centrifugal pumps [NEA/CSNI/R(2013)2], June 2013.
- Collection and analysis of CCF of control rod drive assemblies [NEA/CSNI/R(2013)4], June 2013.
- Collection and analysis of CCF of heat exchangers [NEA/CSNI/R(2015)11], April 2013.
- ICDE Workshop – Collection and Analysis of Common-Cause Failures due to External Factors [NEA/CSNI/R(2015)17], October 2015.
- ICDE Workshop – Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Population [NEA/CSNI/R(2017)8], August 2017.

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) and Mattias Håkansson (ÅF).

In addition, the ICDE Working Group and the individuals with whom they liaise in all participating countries are recognised as important contributors to the success of this study. Olli Nevander was the administrative NEA officer and contributed to finalising the report.

List of tables

List of figures

Executive summary

This report documents a study performed on a set of common-cause failure (CCF) events of Emergency Diesel Generators (EDG) at nuclear power plants. In May 2000, the ICDE Project published a report summarising the collection and analysis of EDG CCF events. The report examined 106 collected events. Since that time, the ICDE Project has continued the collection of EDG CCF events. The database now includes 224 EDG CCF events spanning a period from 1977 through 2012. These events were examined by tabulating the data and observing trends. Once trends were identified, individual events were reviewed for insights. The objectives of this report are:

- To describe the data profile for EDG.
- To develop qualitative insights in the nature of the reported events, expressed by root causes, coupling factors and corrective actions.
- To develop the failure mechanisms and phenomena involved in the events, their relationship to the root causes and possibilities for improvement.

This study presents an overview of the entire EDG data set. The data span a period from 1977 through 2012. The data are not necessarily complete for each country through this period. This information includes root cause, coupling factor, observed population (OP) size, corrective action, the degree of failure, affected subsystem, and detection method. The degree of failure is based on defined severity categories, which are used in the assessment. Charts and tables are provided exhibiting the event count for each of these event parameters. The data in the report was collected according to the internal processes of the participating organisations and checked according to their internal quality assurance programmes. The event information provided by the participating organisations is intended to be analysed within the scope of the project; it is not intended that the event data is changed unless the events undergo a review by the responsible national co-ordinator. The root causes presented in the report are in general not based on a full scope formal root cause analysis.

The analysis of engineering aspects of the events presents a qualitative assessment of the collected data; events are analysed with respect to failure mechanisms and failure cause categories through use of an assessment matrix. In addition, an assessment of complete and partial failures was conducted.

The analysis has resulted in a number of conclusions that can be drawn from this data review. The following notable observations were made.

- The most frequently occurring causes of EDG failures are design errors related to design, manufacture or construction inadequacy.
- Events with failure causes related to deficiencies in operation tend to include a higher proportion of severe failures.

- Maintenance/test was the main way of detecting problems with the diesels, followed by unknown detection methods and test during operation. 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.
- The most common diesel generator failure mechanism category is comprised of ancillary systems, with many failures involving cooling water or fuel supply systems.
- I&C failures are more likely than other types of failure mechanisms to result in severe CCF events that completely fail multiple components in a group.
- Ten per cent of the reported ICDE diesel generator events are complete CCF events. This is the most severe failure category with complete failure of all diesels in the common-cause component group.
- Fifty diesel generator CCF events have been marked as impacting multiple reactor units.

List of abbreviations and acronyms

CCF	Common-cause failure
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee on the Safety of Nuclear Installations (NEA)
DG	Diesel generator
ED	Emergency diesel
EDG	Emergency diesel generator
ENSI	Eidgenössisches Nuklearsicherheitsinspektora (Switzerland)
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
HVAC	Heating, ventilation and air-conditioning
I&C	Instrumentation and control
ICDE	International common-cause failure data exchange
IRS	Incident reporting system
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (France)
KAERI	Korea Atomic Energy Research Institute (Korea)
LOSP	Loss of off-site power
MCC	Motor control centre
M/T	Maintenance/test
NRA	Nuclear Regulatory Authority (Japan)
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission (United States)
OECD	Organisation for Economic Co-operation and Development
OP	Observed population
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
SSM	Swedish Radiation Safety Authority (Sweden)
STUK	Finnish Centre for Radiation and Nuclear Safety (Finland)
UJV	Nuclear Research Institute (Czech Republic)

Glossary

CCF 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 CCF: A CCF 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 CCFs.

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.

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.

ICDE event: Refers to all events accepted into the ICDE database. This includes events meeting the typical definition of CCF event (as described in Appendix B). ICDE events

also include less severe events, such as those with impairment of two or more components (with respect to performing a specific function) that exists over a relevant time interval and is the direct result of a shared cause.

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 CCF 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.

1. Introduction

This report presents an overview of the exchange of common-cause failure (CCF) data of emergency diesel generator (EDG) among several countries. The objectives of this report are:

- To describe the data profile for EDG.
- To develop qualitative insights in the nature of the reported events, expressed by root causes, coupling factors, and corrective actions.
- 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 EDG component. Section 3 presents an overview of the contents of the EDG database and a summary of statistics. 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 International Common-Cause Failure Data Exchange (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 CCFs and the ICDE event definitions. In Appendices C to E, the failure analysis assessments including a short description of each diesel event can be found, comprising of a history describing the observed events and influences leading to the given failure ("the failure mechanism").

2. Component description

This section is extracted from emergency diesel generator (EDG) coding guidelines, which is an appendix to the ICDE general coding guidelines [1]

2.1. General description of the component

EDG are part of the electrical power distribution system providing emergency power in the event of loss of off-site power (LOSP) to electrical buses that supply the safety systems of the reactor plant.

At some plants, emergency diesels (ED) directly drive safety injection pumps and/or emergency feedwater pumps. The EDs/EDGs normally are not in service when the plant is operating at power or shutdown.

The systems for which ED/EDG data are collected are (the corresponding IRS system coding is added in parentheses):

- auxiliary/emergency feedwater (3.BB);
- high pressure and low pressure safety injection (3.BG);
- emergency power generation and auxiliaries, including supply of fuel and lubrication oil (3.EF).

2.2. Component boundaries

The component ED/EDG for this study includes the diesel engine(s) including all components in the exhaust path, electrical generator, generator exciter, output breaker, EDG room heating/ventilating systems including combustion air, lube oil system including the device (e.g. valve) that physically controls the cooling medium, cooling system including the device (e.g. valve) that physically controls its cooling medium, fuel oil system including all storage tanks permanently connected to the engine supply, and the starting compressed-air system. All pumps, valves and valve operators including the power supply breaker, and associated piping for the above systems are included.

Included within the ED/EDG are the circuit breakers, which are located at the motor control centres (MCC) and the associated power boards that supply power to any of the EDG equipment. The MCCs and the power boards are not included except for the load shedding and load sequencing circuitry/devices, which are, in some cases, physically located within the MCCs. Load shedding of the safety bus and subsequent load sequencing onto the bus of vital electrical loads is considered integral to the EDG function and is therefore considered within the bounds of this study. Also included is all instrumentation and control logic (I&C), and the attendant process detectors for system initiations, trips, and operational control.

Ventilation systems and cooling associated with the ED/EDG systems are included, with the exception of the service water system (or other cooling medium) that supplies cooling to the individual ED/EDG related heat exchangers. Only the specific device (e.g. valve) that controls flow of the cooling medium to the individual ED/EDG auxiliary heat exchangers are included. (Complete failure of the service water system that results in failure of the ED/EDGs is normally explicitly modelled under the service water system.)

2.3. Event boundary

The mission for the EDs/EDGs is to 1) start and supply motive force/electrical power in the event of a LOSP and to 2) start and be ready to load in the event of a loss-of-coolant accident. The event boundary is therefore defined as any condition that does not permit the ED/EDG to start or supply motive force/electrical power in the event of loss of coolant or LOSP.

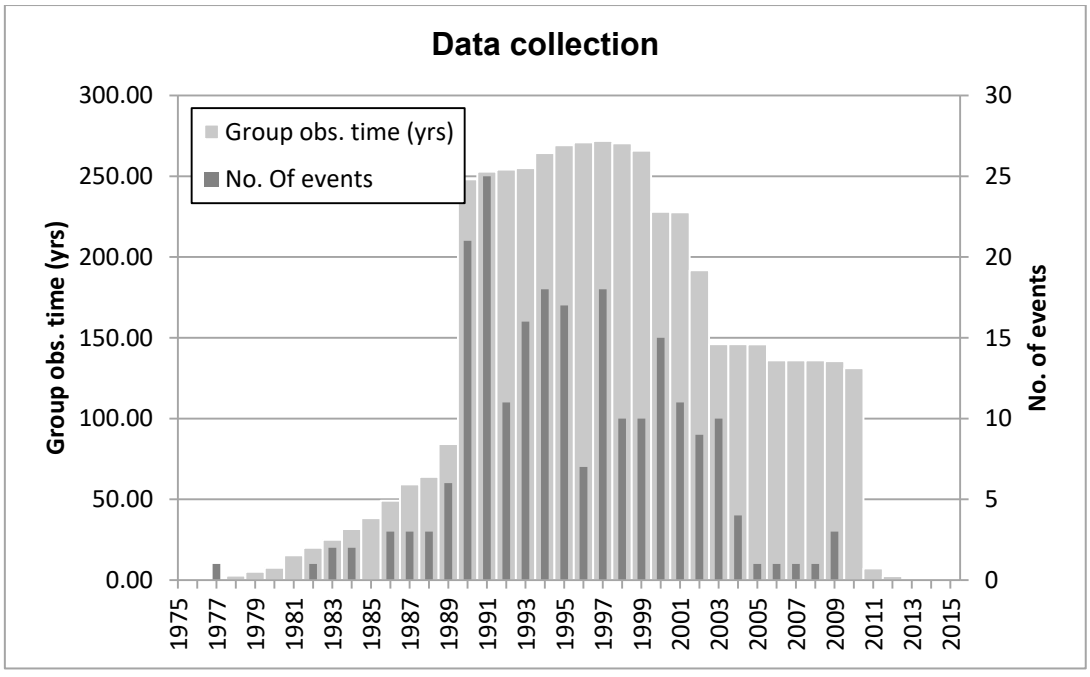
3. Overview of database content

3.1. Overview

CCF data have been collected EDG. Organisations from Canada, Finland, France, Germany, Japan, Korea, Spain, Sweden, Switzerland, the United Kingdom and the United States have contributed to this data exchange. Two-hundred-twenty-nine (229) ICDE events were reported from nuclear power plants (pressurised water reactors, boiling water reactors, Magnox and advanced gas reactors) and the data span a period from 1977 through 2012. However, five events involve emergency gas turbines and these have been excluded, which results in 224 events covered in this report. The data are not necessarily complete for each country throughout this period. Compared with the data covered by the previous published diesel report [2], 118 new diesel events are covered in this report.

The data collection includes 244 reactor units and 4 850 group observation years. **Figure 3.1** presents the data collection of group observation times (years) and number of events distributed over time.

Figure 3.1. Observation time and event count distributed over time



Collecting these events have included both top-down work by identifying events on the basis of licensee event reports and bottom-up work by going through events in plant maintenance databases. Although most CCF events are identified through the former

mechanism, the latter has led to ICDE events that were not identified otherwise. This bottom-up work is rather resource intensive.

The distributions of events in the following section are strictly based on the classes given in the ICDE coding guidelines [1] and as coded by the national co-ordinators. The root causes presented here are in general not based on a full scope formal root cause analysis. In Section 4, a deeper engineering analysis of the events is presented.

3.2. Failure mode and impact of failure

For each event in the ICDE database, the impairment of each component in the OP has been defined according to the categorisation of the general coding guidelines [1] with interpretation as presented in the EDG coding guidelines (see Section 2) and summarised here:

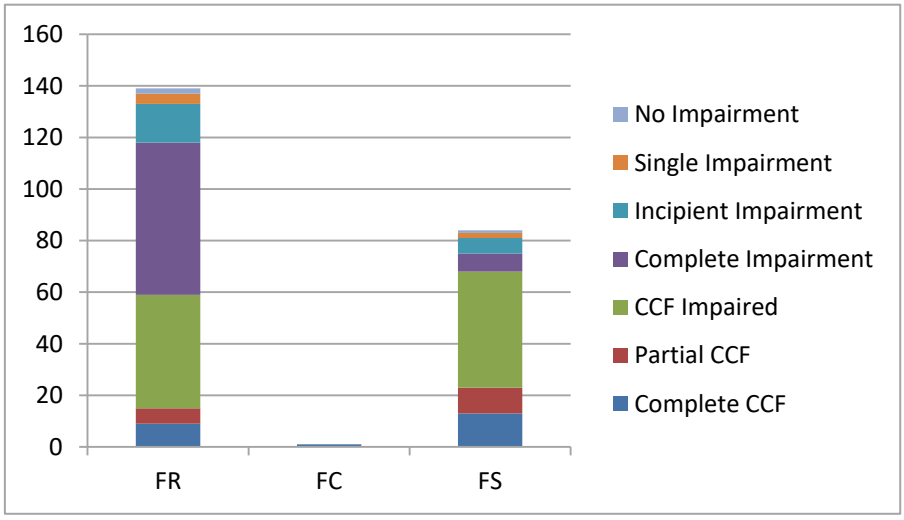
- C denotes complete failure. The component has completely failed and will not perform its function. For example, if the cause prevents an EDG from starting, the EDG has completely failed and impairment would be complete. If the description is vague this code is assigned in order to be conservative.
- D denotes degraded. The component is capable of performing the major portion of the safety function, but parts of it are degraded. For example, reduced capacity of an EDG.
- I denotes incipient. 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. This coding is selected when slight damage is evident. If parts were replaced on some components due to failures of parallel components, this code is used for the components that didn't actually experience a failure. This also applies if it was decided to implement said replacement at a later time.
- W denotes working, i.e. component has suffered no damage. The component is working according to specifications.

Table 3.1 and **Figure 3.1** 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. Twenty-three of the events (10%) were complete CCF events. Complete CCF events are ICDE events in which all components of the exposed population (or observed population respectively) fail completely due to the same cause and within a short time interval. A further subclass of ICDE events are partial CCF events having at least two components, but not all of them, completely failed. The most common failure mode is "failure to run" (62%), followed by "failure to start" (37%).

Table 3.1. Distribution of severity per failure mode

Failure mode	No. of events	Severity category[1]						
		a	b	c	d	e	f	g
Failure to run (FR)	139	9	6	44	59	15	4	2
Failure to stop (FC)	1	1						
Failure to start (FS)	84	13	10	45	7	6	2	1
Total	**224**	**23**[2]	**16**	**89**	**66**	**21**	**6**	**3**

Figure 3.2. Distribution of severity per failure mode



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).
e) Incipient impairment = Multiple impairments but at least one component working. No complete failure. Incomplete but multiple impairments with no C in the impairment vector.
f) Single impairment = The event does not contain multiple impairments. Only one component impaired. No CCF event.
g) No impairment = All components working.
2. One event was originally coded as a complete CCF. It was later assessed to be two events at two different units at one site, each event with component impairment "completely failed and working". It is a multi-unit event (affecting two units). This event is included as complete CCF in Table 3.1, but this event was not marked with the "Complete CCF" interesting event code in Table 4.8.

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 3.2 and **Figure 3.3** show the distribution of the events by root causes.[3] The dominant root cause is "Design, manufacture or construction inadequacy" (D) which accounts for 44% of the failure events. Many of the events with design related root causes involve design errors or construction inadequacy in piece parts for diesel generator ancillary systems, for example the cooling water system, fuel supply systems, and electrical parts. Fifty one per cent of the events with root cause coded as D involve failures of ancillary systems. After ancillary systems, the next highest contribution of design errors involves engine or combustion failures with 24% of the root cause D events.

Most of the events involve design issues with piece parts or sub-systems; however, fundamental design errors in the overall system design can also occur. While this type of serious design error is expected to be rare, there is an example in the ICDE database. A design error led to installation of diesel generators with too low power rating. It was determined that the diesel generators could not provide full emergency design loads. All three diesel generators at the plant were replaced with new units.

Design errors have the potential to impact many plants as some common parts are used across an entire fleet of plants. An example that is found in the database is an improper design (gap rod/valve) in a three-way-valve which controls the cooling system to the diesel causing insufficient cooling. This type of event led to design modification or repair of three-way-valves at 12 different reactor units.

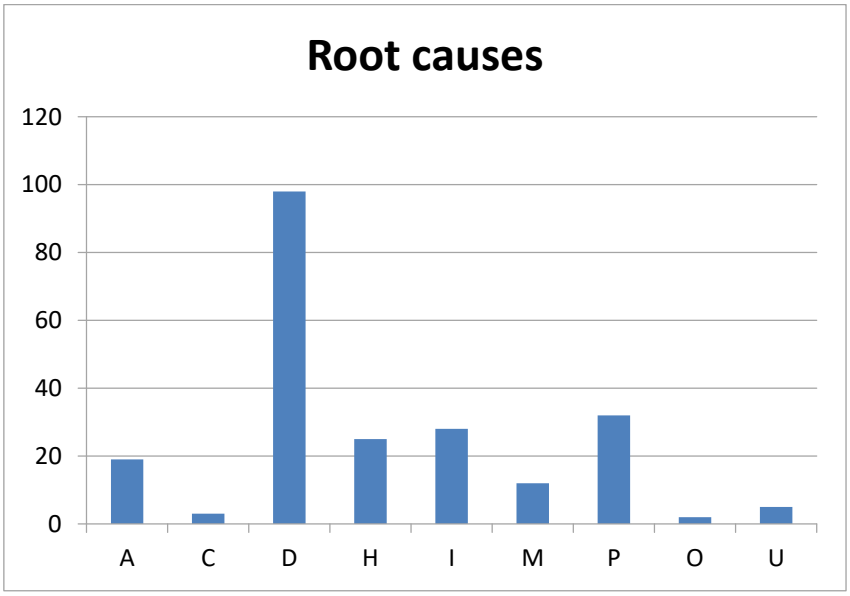
Table 3.2. Distribution of root cause per severity category

Root cause	No. of events	Severity category						
		a	b	c	d	e	f	g
Abnormal environmental stress (A)	19	4	1	5	6	3		
State of other component(s) (C)	3	1	1			1		
Design, manufacture or construction inadequacy (D)	98	5	2	38	35	11	6	1
Human actions, plant staff (H)	25 (24)[4]	6 (5)	6	8	3	1		1
Internal to component or piece part (I)	28	2	4	16	4	2		
Maintenance (M)	12			7	2	2		1
Procedure inadequacy (P)	32	5	2	14	10	1		
Other (O)	2			1	1			
Unknown (U)	5				5			
Total	**224**	**23**	**16**	**89**	**66**	**21**	**6**	**3**

3. The root causes presented here are in general not based on a full scope formal root cause analysis. The coding and identification of root causes is based on the internal processes of the participating organisations and checked according to their internal quality assurance programs. The event information provided by the participating organisations is intended to be analysed within the scope of the project; it is not intended that the event data is changed unless the events undergo a review by the responsible national coordinator.

4. One event occurred during a complex, non-standard plant situation while performing extensive modifications. For this event, the applied coding "Human actions, plant staff (H)" may be regarded as questionable. For the conclusions made in Sections 4 and 5, it is not relevant whether five or six events are assigned to category "H".

Figure 3.3. Distribution of diesel event 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:

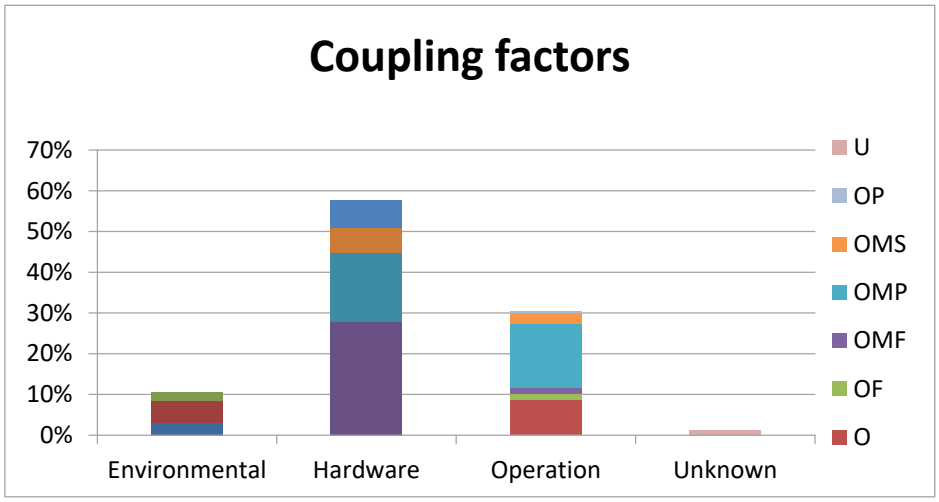
- Environmental: E, EE, EI
- Hardware: H, HC, HS, HQ
- Operation: O, OMF, OMP, OP, OF, OMS

Table 3.4 and **Figure 3.4** 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 3.3. Distribution of coupling factors per severity category

		Severity category						
Coupling factor category	**No. of events**	**a**	**b**	**c**	**d**	**e**	**f**	**g**
Environmental	25	4	1	5	9	6		
Hardware	131	8	7	54	41	13	6	2
Operation	66	11	8	29	15	2		1
Unknown	2			1	1			
Total	**224**	**23**	**16**	**89**	**66**	**21**	**6**	**3**

Figure 3.4. Distribution of diesel event 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 walkdown

MC monitoring in control room

MA maintenance/test

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

TI test during operation

TA test during annual overhaul

TL test during laboratory

TU unscheduled test

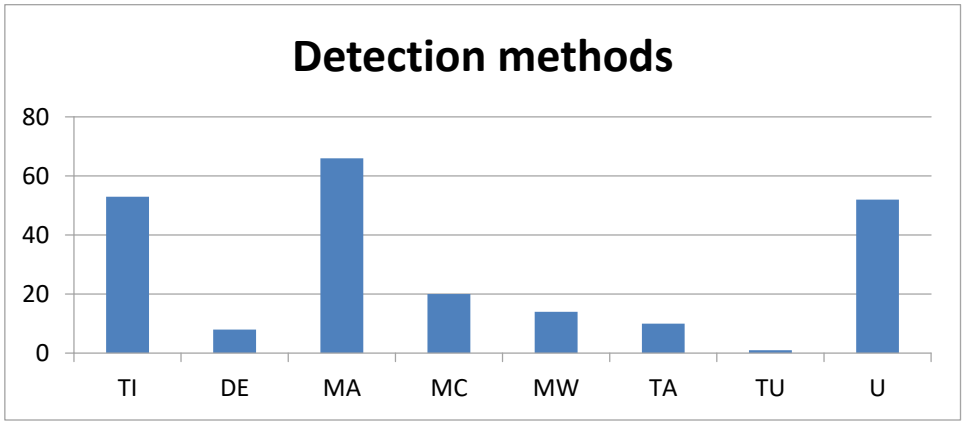
U unknown

Table 3.4 and **Figure 3.5** 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 and test during operation.

Table 3.4. Distribution of detection methods per severity category

Detection methods	No. of events	Severity category						
		a	b	c	d	e	f	g
Test during operation (TI)	53	4	2	33	7	6	1	
Demand event (DE)	8	2		5	1			
Maintenance/test (MA)	66	1	4	20	29	8	3	1
Monitoring in control room (MC)	20	3	4	7	4	1	1	
Monitoring on walkdown (MW)	14	2		1	9	2		
Test during annual overhaul (TA)	10	4		4	1		1	
Unscheduled test (TU)	1							1
Unknown (U)	52	7	6	19	15	4		1
Total	**224**	**23**	**16**	**89**	**66**	**21**	**6**	**3**

Figure 3.5. Distribution of diesel event detection methods



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

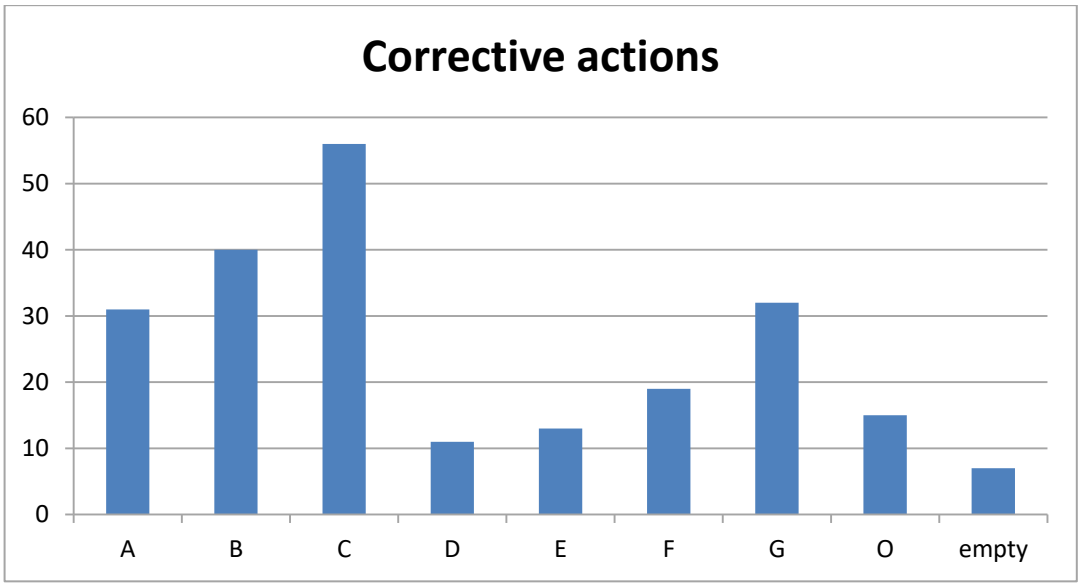
O Other. The corrective action is not included in the classification scheme.

The distribution of the events for corrective actions is shown in **Table 3.5** and **Figure 3.6** . Twenty-five per cent of the corrective actions are made by "Design modifications" (C), followed by "Specific maintenance/operations practices" (B).

Table 3.5. Distribution of corrective actions per severity category

Corrective action	No. of events	Severity category						
		a	b	c	d	e	f	g
General administrative/ procedure controls (A)	31	7	5	12	6	1		
Specific maintenance/ operation practices (B)	40	3	2	15	13	7		
Design modifications (C)	56	1	1	27	17	4	5	1
Diversity (D)	11	3		3	4	1		
Functional/spatial separation (E)	13	2	1	5	4	1		
Test and maintenance policies (F)	19	3	2	10	2	1		1
Fixing of component (G)	32	3	3	11	9	4	1	1
Other (O)	15	1	2	4	6	2		
No Data (empty)	7			2	5			
Total	**224**	**23**	**16**	**89**	**66**	**21**	**6**	**3**

Figure 3.6. Distribution of diesel event corrective actions



4. Engineering aspects of the collected events

4.1. Assessment basis

This section contains an engineering review of the diesel events. The events are analysed with respect to the failure by specifying the failure mechanism description and identifying the failure mechanism category and the failure cause category for each event. In addition, extra ordinary events which are of special interest are marked by specific codes. The failure analysis is performed by the ICDE Project participants during dedicated workshop sessions. The failure analysis assessment allows the ICDE participants to perform an in depth review of the event data from all the participating countries. This failure analysis approach helps the ICDE group develop common insights and trends across the entire data population. The currently applied failure analysis areas are summarised in the Failure Analysis Coding Guide (project internal document) [3] which aims at supporting the analyst during the review. The codes are a result of performed work by the ICDE Steering group. The failure analysis in this report is based on the following definitions extracted from [3].

Failure mechanism description

The failure mechanism is a history describing the observed events and influences leading to a given failure. Elements of the failure mechanism could be a deviation or degradation or a chain of consequences. It is derived from the event description and should preferably consist of one sentence. For example, cracks in numerous relay sockets were induced by vibrations in the EDG rooms resulting failure of diesel load control. The failure mechanism descriptions for all diesel events are presented in Appendix C.

Failure mechanism category

A failure mechanism sub-category is component-type-specific observed faults or non-conformities which have led to the ICDE event and a failure mechanism category is a group of similar failure mechanism sub-categories. E.g. for diesels the failure mechanism sub-categories “Faulty subcomponent”, “Faulty system configuration/Operator control actions” and “Faulty logic” are grouped to the failure mechanism category “misalignment”. In Table 4.1, the six failure mechanism categories and their sub-categories for emergency diesel events are presented.

Table 4.1. Failure mechanism categories and sub-categories

Failure mechanism category and sub-category	
Engine damage or problems (FM1)	
a1	Starting air or air supply valve/distributor damage
a2	(Potential) damage of rotating or stationary parts (bearings, crankcase high pressure in crankcase etc.)
a3	Combustion chamber problems (e.g. cylinder, piston, fuel injection nozzle and pump damage)
a4	Coupling (between engine and generator) damage
a5	Combustion/Charing air problems (e.g. air intake, turbocharger damage)
a6	Other, for example faulty operator action or maintenance error
Compromised ancillary systems (FM2)	
b1	Cooling – missing cooling water or low cooling water pressure (pump unavailable, pipe clogged, pipe or heat exchanger blocked etc.)
b2	Cooling – cooling water temperature (e.g. due to heat exchanger problems) water pipe leaking
b3	Cooling – cooling water leakage (internal/external)
b4	Lubrication – missing lube oil or low lube oil pressure
b5	Lubrication – bad quality or wrong temperature of lube oil
b6	Compromised air intake or cooling of ventilation
b7	Unavailability of or too low pressure in compressed-air system (for diesel start)
b8	Fuel – quantity
b9	Fuel – quality
b10	Fuel – leakage– (internal/external)
b11	Other, for example faulty operator action or maintenance error
Electrical failures (FM3)	
c1	Alternator damage
c2	Breaker/relay failure
c3	Other electrical damage (e.g. of cables, cabinets)
c4	Other, for example faulty operator action or maintenance error
Deficient control and deficient protective cut-out (I&C problems) (FM4)	
d1	Defective or unsuited piece part
d2	Misadjusted set points
d3	Inadvertent actuation of protective cut-out or fire protection system (e.g. due to electromagnetic influence, fume/dust)
d4	Other, for example faulty operator action or maintenance error
Misalignment (FM5)	
e1	Faulty subcomponent
e2	Faulty system configuration/Operator control actions
e3	Faulty logic
Not specified/Others (FM6)	
f1	External/internal hazards (which compromise more than one of the above mentioned component parts at once)
f2	Other, for example faulty operator action or maintenance error

Failure cause category

The codes for failure causes are not component dependent, however, they are dependent on root cause and coupling factor. By definition, it is the coupling factor that identifies the mechanism that ties together multiple failures and the influences that created the conditions for multiple components to be affected. The root cause alone does not provide

the information required for identifying failure cause categories. There are six failure cause categories which are distributed over two types of groups; deficiencies in operation and deficiencies in design, construction and manufacturing:

- Deficiencies in operation
  - O1 Deficient procedures for maintenance and/or testing
  - O2 Insufficient attention to ageing of piece parts
  - O3 Insufficient qualification and/or work control during maintenance/test or operation
- Deficiencies in design, construction, manufacturing
  - D Deficiency in design of hardware
  - C/M Deficiency in construction or manufacturing of hardware
  - D-MOD Deficient design modifications

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. 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.

4.2. Failure analysis assessment matrix

In Table 4.2 the result of the failure analysis is presented in terms of a matrix showing the relationship of failure mechanism and failure cause categories. The failure mechanism categories as defined in Section 4.1 are assigned to the columns of the matrix, the failure cause categories as defined in Section 4.1 are assigned to the rows of the matrix. The matrix entries show the number of ICDE events having been reported for each of the failure mechanism/failure cause combinations.

Here it can be seen that the most common type of observed failure mechanism is compromised ancillary systems (45% of events), followed by engine damage or problems (26%), I&C problems (13%), and electrical failures (12%). The ancillary systems are further divided into sub-categories related to cooling water, fuel supply, lubrication, ventilation, air start and other sub-systems. The most common ancillary system failures involved the cooling water and fuel supply systems. The most common type of diesel failures is caused by failure cause category D, deficiency in design of hardware (39%), followed by failure cause category O1, deficient procedures for maintenance and/or testing (24%).

The failure mechanism category engine damage or problems (FM1) are problems related to cracks or loose parts due to fatigue coming from design issues in particular on connection rods (sub-category a2). Other important issues are related to problems with the fuel injection (sub-category a3) due to leaks or problems with fuel injection pumps. Other important issues are related to (sub-category a1, a4 and a5) start air equipment or combustion air problems due to weather or snow. The majority of these events are

attributed to manufacturing deficiencies. In general, there are low CCF severity for these events.

Many of the events involve failure mechanisms related to compromised ancillary systems (FM2). A large group of event are related to different kind of cooling problems (sub-category b1, b2, and b3) mainly due to design issues leading to contamination, sludge, corrosion, vibrations, leakages, etc. Another large group of events are related to different fuel supply problems (sub-category b8, b9, and b10) mainly due to design issues related to inappropriate fuel pipe support or clamps problems due corrosion or vibrations leading to cracks in the fuel piping. Many of these events are severe events, being complete CCF events or complete impairment event affecting all EDG.

Failure mechanisms related to electrical failures (FM3) are observed with failures of various electrical equipment such as breakers, relays, fuses, tachometers, or governors. Failures related to the alternator (sub-category c1) are rarely observed.

Among the I&C problems (FM4), there are examples of events with faults in the fire protection system, loose parts and connection problems, and electromagnetic interference from switching operations of transformers. Another example of an I&C failure mechanism involved a complete CCF event due to a software design error in the starting system.

Only a small fraction of the events was observed in failure mechanism categories misalignment (FM5) and Not specified/Other (FM6).

Table 4.2. Failure Analysis assessment matrix

Failure cause category	Failure mechanism category						
	Engine damage or problems	**Compro-mised ancillary systems**	**Electrical failures**	**Deficient control or deficient protective cut-out (I&C problems)**	**Misalign-ment**	**Not specified**	**Total**
Deficiencies in operation	**21**	**37**	**13**	**15**	**2**	**6**	**94**
O1	12	25	5	4	2	5	53
O2	7	1	3	1			12
O3	2	11	5	10		1	29
Deficiencies in design, construction, manufacturing	**37**	**63**	**13**	**13**	**3**	**1**	**130**
D	21	47	7	10	2	1	88
C/M	14	8	4	2			28
D-MOD	2	8	2	1	1		14
Total	**58**	**100**	**26**	**28**	**5**	**7**	**224**

4.3. Failure analysis assessment of deficiencies in operation

In **Table 4.3**, it is seen that deficient procedure (O1) is the most common cause of failure among the events assigned to deficiencies in operation, followed by insufficient qualification and/or work control (O3). A summary of each failure cause category related to deficiencies in operation is presented below.

Deficient procedures for maintenance and/or testing (O1)

Examples of failures due to deficient procedures for maintenance and/or testing are given below. These failures often involve issues related to inadequate management of corrosion or fatigue.

- The cooling water check valves and pump shafts and bearings were corroded causing low cooling water flow.
- Pins in the coupling sleeves of pumps used to provide fuel to the EDGs were broken due to mechanical fatigue. These pins had never been replaced since the unit started to operate.

In other examples the cause is directly related to a human error.

- Operators fail to reposition valves to establish cooling water flow after repairs or maintenance.
- Excessive water in the fuel oil system, which resulted from inadequate sampling of the fuel oil storage tank.

Failures due to procedure inadequacies and/or testing are commonly observed in the data. These failures also tend to result in more severe CCF categories. See Section 4.5 for more discussion of the most severe CCF categories, complete and partial CCFs.

Insufficient attention to ageing of piece parts (O2)

Failure cause O2, insufficient attention to ageing of piece parts, has the fewest events among all failure cause categories. Also, this group did not include any events in the most severe failure categories (i.e. complete CCF and partial CCF.) These events tend to evolve slowly over time and can be prevented by an effective ageing management programme.

Insufficient qualification and/or work control during maintenance/test or operation (O3)

Failures caused by insufficient qualification and/or work control is the second most prevalent failure cause category related to operation. Of the 29 events identified with failure cause category O3, eight of these are complete CCFs, with all diesel generators in the group completely failed. Although there are not a large number of events in this cause category, a large proportion of these events are severe failures. This highlights the importance of establishing adequate worker training programmes and appropriate work controls. Also, special attention should be placed on exchanging components and/or piece parts in redundant trains. Staggered replacement should be considered. This is a problem that could affect any type of component whenever replacement is required because life expectancy is about to finish, and original replacements are no longer available in the market.

In some events the cause can include both design and operational aspects. For example, an event occurred where a wrong electrical wiring diagram resulted in wiring errors which led to an increase of the diesels' voltage levels beyond the desired operating band for all diesel generators at a two-unit site. For these events the root cause is coded as D, design, manufacture or construction inadequacy, due to the design error in the wiring diagram. However, the failure analysis performed during an ICDE data workshop assigned failure cause category O3, insufficient qualification and/or work control, to these events.

Failures caused by deficiencies in operations cause many of the events involving I&C failures. In addition to the wiring errors mentioned above, other examples include failures to correctly position relays and misalignment of permissive controls after maintenance and testing. These types of failures are often the most severe, as they can lead to the complete failure of the diesel generators and would require recovery actions if there was a demand for the system.

One high level conclusion that can be drawn is that events with failure causes related to deficiencies in operation tend to include a higher proportion of severe failures.

Table 4.4 provides a summary of the findings in each of the failure assessment matrix categories involving deficiencies in operation.

The failure mechanism descriptions for all diesel events are presented in Appendix C-E.

Table 4.4. Failure analysis assessment matrix findings for deficiencies in operation

Failure cause category	Failure mechanism category						
	Engine damage or problems	**Compromised ancillary systems**	**Electrical failures**	**Deficient control or deficient protective cut-out (I&C problems)**	**Misalignment**	**Not specified**	**Total**
Deficiencies in operation	**21**	**37**	**13**	**15**	**2**	**6**	**94**
O1	Many of the events (5/12) relate to combustion chamber problems (a3). Most deficiencies relate to maintenance procedure (e.g. incorrect torque settings, insufficient cleaning, and introduction of foreign material). (12)	A large group of events (10/25) are related to different kind of cooling problems (b1, b2, and b3) mainly due to procedure errors, such as inadequate operation procedures and improper assembly, but also corrosion and fatigue. Another large group of events (9/25) are related to different fuel supply problems (b8, b9, and b10) mainly due difficulties to read/set the oil/fuel level, but also a few events concern contamination of fuel supply. For a few events, problems relate to lubrication issues. Low severity for many of the events (20/25). (25)	Problems concern breaker/relay failure, e.g. cracks in numerous relay sockets induced by vibrations in the EDG rooms (c2). Another problem is a jammed speed regulator due to little exercise (c3). (5)	Problems relate to wrong/misadjusted settings (d2), inhibited auto-start feature, and insufficient torqued screw (d4). (4)	Problems relate to faulty system configuration/ operator control actions due to human error (e2). (2)	Problems relate to errors in test procedures. Events led to complete CCF for 3/5 events (f2). (5)	53
O2	Problems relate to ageing of piece parts in the air supply system (a1), the solenoid start-up valves (a3), and degraded engine to generator coupling (a4). Low severity for all events, i.e. no partial or complete CCF. (7)	Problem relate to dehydration causing cracks in fuel hose (b10). (1)	Problems relate to long term heat fatigue of the resistors in the governor unit (c3). (3)	Defective spare part which led to failed connection between the oil supply and the speed controller (d1). (1)			12
O3	Problems relate to error during maintenance that led to low exhaust temperature (a3), and a glazed clutch which caused the engine to trip on overspeed (a4). (2)	Problems relate to lubrication deficiencies (b4), comprised air intake (b6), fuel oil supply (b10), and clogging of cooling water heat exchangers (b1). Other problems relate to insufficient work control (human error) (b11). Several events (4/8) with high severity. (11)	Problems relate to breaker/relay failures (c2), broken/cut-off cables (c3), and use of unsuited equipment (c4). (5)	Most of the problems relate to wiring errors and human errors (d4). Other problems relate to unsuited parts (d1), misalignment (d2), and spurious operation of relays (d3). (10)		Problem relate to requalification testing and lack of safety culture (operator staff poorly trained). (1)	29

4.4. Failure analysis assessment of deficiencies in design, construction and manufacturing

Deficiency in the design of hardware is the most important cause category dominated by compromised ancillary systems. Many of the failures of ancillary systems involve cooling water systems or fuel supply systems. Most of the ancillary system failures are caused by deficiencies in design, construction and manufacturing of hardware. Some examples of these types of hardware related failures are discussed below.

- A small leak in a fuel supply pipe due to failure to account for vibration resistance in the piping system design.
- The materials selected for a cooling water system pipe and flange resulted in electrical potential between different materials ultimately leading to corrosion and leaking of the cooling water pipes.

The examples given above demonstrate failures due to hardware design errors. These highlight the importance of adequate design for all anticipated operating conditions. This is particularly important for such a complex component that relies on several ancillary systems.

Engine problem is another contributing factor mainly related to design issues or construction and manufacturing. Examples of such issues are:

- Cracks found in fuel injector nozzles due to inadequate design and manufacturing.
- Cracks in connecting rods due to fatigue.
- Failure to start due to air valves problems in the start air system.
- Combustion air intake problems due to severe weather.
- Turbocharger problems due to resonance.

Electrical failures and I&C problem are also represented among the events. Examples of such events are:

- Speed/tachometer problems.
- Component protection problems.
- Load governor problems.

Table 4.5 provides a summary of the findings in each of the failure assessment matrix categories involving deficiencies in design, construction, and manufacturing.

Table 4.5. Failure analysis assessment matrix findings for deficiencies in design

Failure cause category	Failure mechanism category						
	Engine damage or problems	**Compromised ancillary systems**	**Electrical failures**	**Deficient control or deficient protective cut-out (I&C problems)**	**Misalignment**	**Not specified**	**Total**
Deficiencies in design, construction, manufacturing	**37**	**63**	**13**	**13**	**3**	**1**	**130**
D	Problems relate to cracks or loose parts due to fatigue coming from design issues in particular on connection rods (a2). Other problems relate to the fuel injection due to leaks or problems with fuel injection pumps (a3). Other important issues are related to start air equipment or combustion air problems due to weather, snow (a1, a4 and a5). In general, there are low CCF severity for these events. (21)	A large group of events are related to different kind of cooling problems (b1, b2, and b3) mainly due to design issues leading to contamination, sludge, corrosion, vibrations, leakages, etc. Another large group of events are related to different fuel supply problems (b8, b9, and b10) mainly due to design issues related to inappropriate fuel pipe support or clamps problems due corrosion or vibrations leading to cracks in the fuel piping. Many of these events are severe events, being complete CCF events or complete impairment events affecting all EDG. Design problems related to oil supply are not so important compared to cooling and fuel issues. (47)	The observed events relate to problems in various electrical equipment such as fuses, tachometers, governors etc. Design problems related to the alternator or breakers are not so important (no events). (7)	The I&C problems relate to faults in the fire protection system (incorrect signal and blown fuses [complete CCF]). In three events, the problems relate to loose parts and connection problems. In one event electromagnetic interference from switching operations of transformers led to faulty overspeed protection signals (d3). In total, two complete CCF and one partial CCF. The other complete CCF was due to software design error in the starting system. (10)	Problems relate to faulty system configuration (e2) and faulty logic (repair work caused a spurious signal) (e3). (2)	Problem related to underrated EDGs. (1)	88
C/M	Majority of the events (9/14) attributed to manufacturing deficiencies but with low severity, meaning no complete or partial CCF. A couple failure mechanisms are developing over time due to vibrations. (14)	4 events with similar FM descriptions (rainwater accumulation in the EDG building leading to leaks in cooling water pipes) with low severity. 2 different sites were affected and events occurred between 1991 and 2002 (lack of experience feedback). (8)	All four events relate to breaker or relay failures (c2). (4)	Deficient subcomponents caused high contact resistance (d1). (2)			28
D-MOD	Design modification of the turbo of the diesel generators resulted in resonance vibrations and failure of the diesels (a5). (2)	All eight events relate to problems with one subcomponent (three-way valve) in a series of plants that was affected by several different problems (b2). The valve controls the cooling system to the diesel. (8)	Two breaker failures, one due to an unsuited spring and one due to early ageing due to change of the power supply voltage. (2)	Error when changing the instrumentation led to overestimation of the diesel fuel tank level (d2). (1)	Diesel generator not able to reach design load due to misadjusted engine governor output linkage (e2). (1)		14

4.5. Failure analysis assessment of complete and partial CCF events

The CCF complete event category is also important for understanding plant risk, as these events represent the most severe type of CCF events where all components in a CCF group are completely failed. Examples of complete CCF events include:

- Due to a failure of a microprocessor associated with the EDG load sequencer circuitry, the EDGs failed to automatically load safety-related loads during testing. If an actual demand would have occurred, then operator action may have been required to manually sequence the emergency loads.
- Sandblasting in the area caused pollution of the air intake for both EDGs. The impact of the in the air distribution system was discovered during testing and it was determined that both EDGs would not be able to fulfil their safety function.

Table 4.7 shows the failure analysis matrix with only the two highest severity event categories: Complete CCF and partial CCF. From the table it is seen that events with failure causes related to deficiencies in operation tend to include a higher proportion of severe failures. Twenty six of the 39 severe events (67%) are caused by deficiencies in operations. This is also seen in Table 10, where human actions and procedure inadequacy is more common than hardware failures. Considering the distribution of failure mechanisms, the highest contribution category is compromised ancillary systems (41%) followed by I&C problems (26%). There are only 28 total events that involved I&C failures (as shown in Table 4.7), and ten of these are high severity categories. So, I&C failures appear more likely than other types of failure mechanisms to result in severe CCF events that completely fail multiple components in a group. **Table 4.6** provides the failure mechanism descriptions for, distributed according to the failure assessment matrix.

Table 4.7. Distribution of root causes for the complete and partial CCF events.

Root cause	Complete CCF	Partial CCF	Total
Abnormal environmental stress (A)	4	1	**5**
Design, manufacture or construction inadequacy (D)	5	2	**7**
Human actions (H)	6	6	**12**
Internal to component, piece part (I)	2	4	**6**
Procedure inadequacy (P)	5	2	**7**
State of other component (C)	1	1	**2**
Total	**23**	**16**	**39**

Table 4.8. Failure analysis assessment matrix for complete and partial CCF events

	Failure Mechanism Category						
Failure Cause Categories	**Engine damage or problems**	**Compromised ancillary systems**	**Electrical failures**	**Deficient control or deficient protective cut-out (I&C problems)**	**Misalignment**	**Not Specified**	**Total**
Deficiencies in operation	**1**	**12**	**3**	**6**	**1**	**3**	**26**
O1	1	5	1	2	1	3	13
O2							0
O3		7	2	4			13
Deficiencies in design, construction, manufacturing	**2**	**4**	**2**	**4**	**1**		**13**
D	1	4	1	3	1		10
C/M			1				1
D-MOD	1			1			2
Total	**3**	**16**	**5**	**10**	**2**	**3**	**39**

Table 4.9. Failure analysis assessment findings for complete and partial CCF events

	Failure mechanism category					
	Engine damage or problems	**Compromised ancillary systems**	**Electrical failures**	**Deficient control or deficient protective cut-out (I&C problems)**	**Misalignment**	**Not Specified**
Deficiencies in operation	(1)	(12)	(3)	(6)	(1)	(3)
O1	• EDGs tripped when released from emergency mode due to foreign material in check valves. These check valves prevent reverse flow from the shutdown control airline into the reset airline. (1)	• EDGs were considered inoperable due to leakage of jacket cooling water. The cause of cracks in the cooling water nipples were attributed to vibration induced fatigue. • Inadequate flow to diesel generator service water heat exchangers due to operator error in repositioning the heat exchanger inlet valves. • Instructions for checking the lube oil level were not specified in the maintenance pro-cedures, which led to low lube oil level. • Mechanical fatigue causing pin rupture in pumps that provide fuel to diesels. • Valve for cooling water not opened again after repair causing high water temperature. (5)	• cracks in numerous relay sockets were induced by vibrations in the EDG rooms resulting failure of diesel load control. (1)	• Low voltage due to insufficient torqued screw in a connection block prevented start of DG. • The auto-start feature for both EDGs was inhibited due to poor procedures for I&Cs testing. (2)	• Diesels were taken out of service which was against the station operation procedure. (1)	• Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply. • Test procedure which erroneously required locking of automatic start-up of both EDGs was not corrected due to a lack of monitoring in procedure modifications. • Complex procedure over-loaded by handwritten remarks led to reconnect a diesel without complete requalification test and to erroneously disconnect a diesel on another unit. (3)
O3		• Paint overspray on the DG exciter commutator ring (cause: management deficiency resulting from inadequate work control and management interface). • Incorrect installation of the service water flow control valves due to procedural inadequacies, inattention to detail and inadequate skills. • 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. • Pollution of the air supply due to sandblasting outside the diesel building led to scoring in the sleeves of the cylinders and to high pressure in the motors. • A large school of fish in the cooling water intake results in clogging of EDG heat exchangers. • Fuel oil leaks on EDG fuel supply lines due to improper fittings. (7).	• Control cable cut off by worker, loss of monitoring. • High resistance of breaker contacts due to hardening of contact lubricant grease. This led to auto-start being inhibited. (2)	• The relay wiring configuration related to EDG output breakers had been designed and installed based on an incorrect print. • Unit trip relays were reset due to operator error preventing EDGs to pick up load when started. • 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 two diesels. • Spurious operation of two diesel generators because of a failed coil of a relay. (4)		

Deficiencies in design, construction, manufacturing	(2)	(4)	(2)	(4)	(1)	
D	• Event description too sparse. (1)	• 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. • Erroneous closing of sea water gates invoked large amounts of sludge movement which blocked the sea water heat exchangers. • Coupling pins failure led to loss of fuel supply preventing the EDG to start. • 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. (4)	• Short circuits in two diodes in the rectifier bridge caused a protective fuse to blow, which resulted in failure of the EDGs to produce the expected voltage. (1)	• Misoperation of the digital time sequencer for automatic loading due to inadequate design. • Design deficiency in the carbon dioxide fire protection system auxiliary circuitry caused a fuse to blow. • Modification to 110V dc system led to incorrect fuses being used on the diesel system leading to failure to run. (3)	• A repair work at the reactor protection system cubicle caused a spurious signal that started the DGs. DGs stopped when the signal disappeared and were unavailable for about 2 minutes. (1)	
C/M			• Lockout relay of both EDG output breakers were found sticking (not tripping when required). (1)			
D-MOD	• A design modification in the turbocharger of EDGs resulted in resonance vibrations during operation and failures of fan blades. (1)			• Error when changing the instrumentation led to overestimation of the diesel fuel tank level. (1)		

4.6. Interesting events – discussion and examples

In Table 4.10, the result of the failure analysis is presented in terms of a marking of interesting events. As part of the ICDE failure analysis process, the project members use the interesting CCF event codes to highlight those ICDE events that have some extraordinary aspects or provide significant insights. Some noteworthy observations include: 50 events (22% of diesel events) are marked as multi-unit events, 10% of events are complete CCFs (i.e. complete failure of all components), 8% of events resulted a major modification, and 6% of events involved a new failure mechanism.

The ICDE interesting CCF event codes may be helpful for identifying or weighting events for CCF quantification. The codes can help to identify the applicability of events to certain types of failures that may be of interest for PSA applications, for example identifying multi-unit events.

Table 4.10. Applied interesting event codes

Interesting CCF event code	Description	No. of events	Percentage
Complete CCF	Event has led to a complete CCF.	22[5]	10%
CCF outside planned test	The CCF event was detected outside of normal periodic and planned testing and inspections.	12	5%
Component not capable	Event revealed that a set of components was not capable to perform its safety function over a long period of time.	9	4%
Multiple defences failed	Several lines of defence failed.	2	1%
New failure mechanism	Unattended or not foreseen failure mechanism.	14	6%
CCF sequence of different CCF	Events with a sequence of different CCF failures and /or subtle dependencies.	0	0%
CCF causes modification	Event causes major modification, e.g. exchange of diesel.	19	8%
Multiple systems affected	Events were a single CCF failure mechanism affected multiple systems.	2	1%
Common Cause Initiator	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.	0	0%
Safety culture	The reason why the event happened originates from safety culture management. Understanding, communication and management of requirements have failed.	9	4%
Multi-unit CCF	CCF affecting a fleet of reactors or multiple units at one site.	50	22%
No code applicable	Indicates that event has been analysed but none of the above codes is applicable.	98	44%
Total no. applied codes		**237**	**-**

5. One event was originally coded as a complete CCF. It was later assessed to be two events at two different units at one site, each event with component impairment "completely failed and working". It is a multi-unit event (affecting two units). This event is included as complete CCF in **Table 3.1**, but this event was not marked with the "Complete CCF" interesting event code in **Table 4.8.**

Some noteworthy aspects of the interesting event assessment are discussed below.

- CCF outside planned test: most of these events were detected by walkdown. Half of the events are correlated to problems with fuel supply: vibration/corrosion causing cracks/leaks in fuel supply and problems in filling the day tanks. Three events were related to problems with the diesel control systems.
- Component not capable: many of the events are related to wrong temperatures due to cold weather, insufficient ventilation or low cooling water flow.
- New CCF mechanism: one example of a not foreseen failure mechanism is an event where the switching operation of transformers led to electromagnetic interference causing tripped tachometer and over speed protection of diesels. Another example is where the turbos of diesel generator units were replaced and 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. Many of the other events are due to external environmental factors (e.g. weather conditions).
- CCF causes modification: there are 19 events identified that resulted in a major modification. One example is the design error which resulted in too small diesel generators being installed at the plant, and all the diesel generators had to be replaced with new units. Another event describes how heavy snow and turbulent winds resulted in blocking of the air filters for the diesel generator air intake. A design modification of the air intake was implemented to avoid blocking again.
- Multi-unit CCF events: the multi-unit CCF events of diesel generators are very important for understanding multi-unit plant risk and developing site-level PSA. Most LOSP initiating events are expected to impact all units at a site, and EDGs would be demanded to respond to such events. There are many examples of multi-unit CCF events in the database. Some events impact units at different sites across a fleet. For example, the three-way valve failures discussed in Section 3.3. Other events are limited to multiple units at a single site. Examples of these site-level events include:
  - Cracks were found in numerous relay sockets that prevented EDGs from starting. The cracks were induced by vibrations, and all sockets were replaced on both units at the site.
  - A diesel generator experienced speed oscillations due to a failed resistor in the governor unit. The same resistor had failed on an EDG in the other unit at the site a few weeks earlier.
  - Miscalibration of diesel fuel storage tank level led to an insufficient fuel supply for all EDGs at the site.
- Safety culture: nine events are marked with the interesting event code related to safety culture. These events demonstrate the importance of prioritising safety in all aspects of the plant operation. Some of these events involve a sequence of multiple human errors. For example, an error in a routine test procedure resulted in a diesel generator failure followed by an inadequate process to review and correct the procedure. Even after 14 months the procedure had not been corrected and the same failure occurred again. Also, one third of the safety culture events resulted in complete CCFs.

4.7. Other topical aspects – EDG CCFs impacting entire exposed populations

The published topical report *ICDE Workshop on EDG CCFs Impacting Entire Exposed Population* [4] examines a subset of data that is covered in this report. The report summarises the analysis of diesel generator CCF events impacting the entire exposed populations, so called "all affected" diesel failures. Many of the same conclusions can be drawn from both reports. The root cause category D, design, manufacture or construction inadequacy, is the most common for the "all affected" data. One notable feature of the data is that the root cause code H, human actions, plant staff, is more prevalent in the most severe failures (severity categories a and b).

The "all affected" report also notes suggested improvements. "Maintenance or testing of component" is the most common area of improvement.

5. Summary and conclusions

Organisations from Canada, Finland, France, Germany, Japan, Korea, Spain, Sweden, Switzerland, the United Kingdom and the United States contributed common-cause failure (CCF) data of EDGs to this data exchange. Two hundred twenty four ICDE events were analysed from nuclear power plants in these countries.

These reported ICDE events were reviewed in Sections 3 and 4 of this report with respect to the degree of failure, failure causes and failure mechanisms. A number of conclusions can be drawn from this data review. The following notable observations are made:

- The most frequently occurring causes of EDG failures are design errors related to design, manufacture or construction inadequacy (root cause category D of ICDE).
- Events with failure causes related to deficiencies in operation tend to include a higher proportion of severe failures.
- Maintenance/test was the main way of detecting problems with the diesels, followed by unknown detection methods and test during operation. 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.
- The most common diesel generator failure mechanism category is comprised of ancillary systems, with many failures involving cooling water or fuel supply systems.
- I&C failures are more likely than other types of failure mechanisms to result in severe CCF events that completely fail multiple components in a group.
- Ten per cent of the reported ICDE diesel generator events are complete CCF events. This is the most severe failure category with complete failure of all diesels in the common-cause component group.
- Fifty diesel generator CCF events have been marked as impacting multiple reactor units.

For the events caused by root cause “Design, manufacture or construction inadequacy” with 44% of the events, many of the events involve design issues with piece parts or sub-systems, but fundamental design errors in the overall system design can also occur. Design has to take into account extreme weather conditions and water chemistry of the external cooling water. Switching operation of high voltage switches can lead to electromagnetic interference in the I&C systems.

Maintenance/test was the main way of detecting problems with the diesels, followed by unknown detection methods and test during operation. 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. Walk-downs and surveillance are important to detect beginning impairments, for example, small leakages in fuel supply.

Design modification related corrective actions have been taken by the utilities in consequence of 25% of the ICDE events; this is in correlation with the large number of failures which are caused by design deficiencies in either the diesel generator or other components that affect the operation of the diesel generator.

The most common type of diesel generator failure mechanism is comprised ancillary systems with 45% of events marked with this failure mechanism category. The event failure mechanisms are further divided into sub-categories related to cooling water, fuel supply, lubrication, ventilation, air start and other sub-systems. The most common ancillary system failures involved the cooling water and fuel supply systems. Other observed failure mechanism categories include engine damage or problems (26% of events), I&C problems (13%), and electrical failures (12%).

For the two highest severity event categories, complete CCF and partial CCF, failure causes related to deficiencies in operation tend to include a higher proportion of severe failures. Twenty six of the 39 severe events (67%) are caused by deficiencies in operations. Also, the I&C failures are more likely than other types of failure mechanisms to result in severe CCF events that completely fail multiple components in a group.

Among the "other interesting events", three categories stand out, CCF causes modification, Multi-unit CCF events and Safety culture.

There are 19 events identified that resulted in a major modification. One example is a design error which resulted in too small diesel generators being installed at the plant, and all the diesel generators had to be replaced with new units.

The multi-unit CCF events of diesel generators are very important for understanding multi-unit plant risk and developing site-level PSA. Most LOSP initiating events are expected to impact all units at a site, and EDGs would be demanded to respond to such events. There are many examples of multi-unit CCF events in the database (50 events). Some events impact units at different sites across a fleet. Other events are limited to multiple units at a single site.

The nine events marked with the interesting event code related to safety culture demonstrate the importance of prioritising safety in all aspects of the plant operation. Some of these events involve a sequence of multiple human errors. There are some safety culture events as examples of inadequate process to prioritise the actions to review and correct the procedures and working methods based on their safety relevancies. Also some of examples are related to missing training of personnel to understand, communicate, prioritise and manage safety requirements.

6. References

1. International Common-Cause Failure Data Exchange ICDE General Coding Guidelines – Updated Version [NEA/CSNI/R(2011)12], October 2011.
2. Collection and analysis of common-cause failure of emergency diesel generators [NEA/CSNI/R(2000)20], May 2000.
3. Failure analysis coding guideline rev 8, February 2016, not published (planned to be included in next revision of ICDE General Coding Guidelines as Appendix 1).
4. ICDE Workshop – Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Population [NEA/CSNI/R(2017)8], August 2017.

7. APPENDIX A – Overview of the ICDE Project

Appendix A contains information regarding the ICDE Project.

Background

Common-cause failure (CCF) events can significantly impact the availability of safety systems of 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 ICDE Project was initiated in August of 1994. Since April 1998 the NEA has formally operated the project, following which the project was successfully operated over six consecutive terms from 1998 to 2014. The current phase started in 2015 and is due to run until end of 2018. Member countries under the current Agreement of NEA and the organisations representing them in the project are: Canada (CNSC), the Czech Republic (UJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), Korea (KAERI), Spain (CSN), Sweden (SSM), Switzerland (ENSI) and the United States (NRC).

More information about the ICDE Project can be found on the NEA website: www.oecd-nea.org/jointproj/icde.html . Additional information can also be found at the website https://projectportal.afconsult.com/ProjectPortal/icde.

Scope of the ICDE Project

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

Data Collection Status

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

ICDE Coding Format and Coding Guidelines

Data collection guidelines have been developed during the project and are continually revised. They describe the methods and documentation requirements necessary for the development of the ICDE databases and reports. The format for data collection is described in the general coding guidelines and in the component specific guidelines.

Component specific guidelines are developed for all analysed component types as the ICDE plans evolve [1].

Protection of Proprietary Rights

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

8. APPENDIX B – Definition of common-cause events

In the modelling of CCFs 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:'

CCF 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 interval. 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 direct result of a shared cause. Thus, in the ICDE Project, we are interested in collecting complete CCF events as well as partial CCF events. The ICDE data analysts may add interesting events that fall outside the CCF event definition but are examples of recurrent – eventually non-random – failures. With growing understanding of CCF events, the relative share of events that can only be modelled as "residual" CCF events is expected to decrease.

9. APPENDIX C – Failure analysis matrix – Deficiencies in operation

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM1	a1	CCF Impaired	P	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.
			CCF Impaired	P	Too much torque on the nuts caused fractured surface on the pin bolts in the start air valve, which led to overstrained pin bolts.
		a2	Complete Impairment	P	Deformed cover lids in the crankcase ventilator led to increased crankcase pressure.
			No Impairment	D	Defective rod bearing.
		a3	CCF Impaired	I	EDG Exhaust Valves Sticking and Broken.
			CCF Impaired	P	Lock-nut of the injection limiter not set properly due to insufficient manufacturer specifications led to a delayed EDG start.
			CCF Impaired	P	Deformation of the fuel pipe line led to leakage and the diesel was stopped due to the risk of fire.
			Complete Impairment	P	Sandblast cleaning of the combustion air intercoolers caused sand to be introduced into the engines and then scoring of cylinder liners and piston rings.
			Incipient Impairment	M	The fuel pump was affected by vibrations which made the fuel ignition occur at the time when the exhaust valves were open.
		a5	Partial CCF	I	EDGs tripped when released from emergency mode due to foreign material in check valves. These check valves prevent reverse flow from the shutdown control air line into the reset air line.
		a6	CCF Impaired	P	Particles from seal tape which was used to fix screws during maintenance were introduced in the speed governor of the EDGs and blocked the motion of the pilot valve plunger.
			Incipient Impairment	C	Leaking lube oil check valves cause EDGs to be inoperable due to valves failing to fully seat after testing.
	FM2	b1	CCF Impaired	D	Cooling water check valves and pump shafts and bearings were worn due to corrosion and normal wear. The pumps would have operated in spite of the vibration but the sticking check valves prevented or decreased the cooling water flow.

1. FCC = Failure cause category, see Section 4.1
2. FM Cat = Failure mechanism category, see Section 4.1
3. FM Sub = Failure mechanism sub-category, see Section 4.1
4. See Section 3.1 for the definitions of event severities.
5. See Section 3.3for the acronyms of root causes.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			CCF Impaired	P	Air intrusion into the cooling water pump due to inadequate operation procedures and piping layout led to a shutdown of the diesel due to low cooling water pressure.
			Partial CCF	H	Valve for cooling water not opened again after repair causing high water temperature.
		b2	Complete Impairment	A	Tube sheet blockage (primarily corrosion nodules) found in the EDG (environmental issue).
			Complete Impairment	P	Improper strainer assembly which lead to stress on welds and damaged strainer basket + cross-connection of strainers -> causing clogging of both cooling water trains to DGs.
			Complete Impairment	P	Improper strainer assembly which lead to stress on welds and damaged strainer basket + cross-connection of strainers -> causing clogging of both cooling water trains to DGs.
			Complete Impairment	P	The rod lock-nut was unscrewing which led to incorrect stroke of the three-way valve in the engine water cooling system.
			Incipient Impairment	P	The diesel failed a surveillance test and was manually tripped. Elevated temperatures and frequency swings were observed. Clogging of the heat exchangers by zebra mussels was the cause of the high temperatures.
			Partial CCF	P	Inadequate flow to diesel generator service water heat exchangers due to operator error in repositioning the heat exchanger inlet valves.
		b3	Partial CCF	A	EDGs were considered inoperable due to leakage of jacket cooling water. The cause of cracks in the cooling water nipples were attributed to vibration induced fatigue.
		b4	Complete Impairment	D	Too low sump oil level and incorrect reading of dipsticks causing loss of lubrication causing gearbox failure.
			Partial CCF	P	Instructions for checking the lube oil level were not specified in the maintenance procedures, which led to low lube oil level.
		b7	CCF Impaired	D	Insufficient lubricant caused the start-up air valves to open too slow.
			CCF Impaired	P	Inadequate test procedure resulted in damage of the air start distributer.
		b8	CCF Impaired	H	Due to difficulties in reading the dipstick when the diesel is running it was not discovered that the oil level was low and hence the diesel generator stopped.
			CCF Impaired	P	EDG fuel oil transfer pump when day tank level was below start set point due to a failed low level cut-out switch. The second EDG fuel oil transfer pump failed due to a blown control power fuse making both EDGs unavailable for auto-start.
			Complete CCF	P	Mechanical fatigue causing pin rupture in pumps that provide fuel to diesels.
			Complete Impairment	D	Inaccurate level instrumentation + human error (not responding to alarm) causing too small fuel level margin without knowing.
			Complete Impairment	M	Wrong calibration of fuel storage tank level could have led to unavailability of the DGs.
		b9	CCF Impaired	P	Loss of lubrication capacity of the fuel injection pump of DG due to the use of inadequate diesel fuel (low sulphur).
			Complete Impairment	P	Both EDGs Inoperable Due To Excessive Water in The fuel Oil System Which Resulted From An Inadequate Sampling Of The Diesel Fuel Oil Bulk Storage Tank.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
		b10	CCF Impaired	M	Re-using of piece part that needs to be replaced during maintenance led to fuel leakage. (Root cause unknown: maintenance documentation or execution?)
			Complete Impairment	H	Leak in bulk storage tank leads to isolation of tank. Which leads to automatic draining of day tank not possible. Excessive fuel contaminated the cam-box lubricating oil of the DGs.
		b11	CCF Impaired	H	improper greasing of fuel oil pump motor bearings rendered pumps inoperable during extremely cold weather conditions.
			CCF Impaired	P	Control power fuses were blown on EDG jacket water system due to poor maintenance practices and less than adequate documentation.
	FM3	c2	CCF Impaired	I	Failure to close of the output breaker led to failure to synchronise the generator to offsite power.
			Complete CCF	A	Cracks in numerous relay sockets were induced by vibrations in the EDG rooms resulting failure of diesel load control.
			Complete Impairment	A	Cracks in numerous relay sockets were induced by vibrations in the EDG rooms could result in failure of diesel load control.
		c3	CCF Impaired	P	Jammed speed regulator due to little exercise causing tripped diesel.
			CCF Impaired	P	Jammed speed regulator in fuel pump causing insufficient speed in order to start diesels.
	FM4	d2	CCF Impaired	O	Failure due to wrong setpoint of overspeed protection.
			Single Impairment	D	Misadjusted settings of the fuel amount governor led to fluctuations of the rotation speed in the start-up process and thereby to the shut-off of the diesel.
		d4	Partial CCF	H	Low voltage due to insufficient torqued screw in a connection block prevented start of DG.
	FM5	e2	CCF Impaired	H	EDGs observed in underspeed condition due to inadequate maintenance on governor replacement and adjustment and inadequate post-maintenance testing.
			Complete CCF	H	Diesels were taken out of service which was against the station operation procedure.
	FM6	f1	CCF Impaired	A	Over temperature 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.
		f2	Complete CCF	H	Complex procedure overloaded by handwritten remarks led to reconnect a diesel without complete requalification test and to erroneously disconnect a diesel on another unit.
			Complete CCF	P	Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply.
			Complete CCF	P	Test procedure which erroneously required locking of automatic start-up of both EDGs was not corrected due to a lack of monitoring in procedure modifications.
			Complete Impairment	P	Locking of automatic start-up of both EDGs were erroneously required by the test procedure on another component.
O2	FM1	a1	CCF Impaired	D	Aged, swelled O-Ring at an pilot valve seals prevented the main starter valve from opening.
			CCF Impaired	D	O-ring of valve piston has aged and hardened, which lead to the failure of both redundant starter valves providing compressed air to the compressors.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			CCF Impaired	P	Fatigue due to ageing caused a valve seat in the high-pressure part in the compressor to crack and small pieces of material were missing (holes in pressure valve disc) which led to failure of the start air compressor.
		a3	CCF Impaired	M	Ageing of toric joints in the start-up solenoid valves.
			CCF Impaired	M	Ageing of toric joints in the start-up solenoid valves.
			Incipient Impairment	M	Ageing of toric joints in the start-up solenoid valves.
	FM2	b10	CCF Impaired	P	Dehydration causing cracks in fuel hose.
	FM3	c1	CCF Impaired	A	Lack of ventilation and Inadequate cooling in excitation cabinet led to DG failure to continue running.
		c3	CCF Impaired	A	Failure of DG is due to failed resistor in the governor unit due to long term heat fatigue.
			CCF Impaired	A	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.
	FM4	d1	CCF Impaired	I	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.
O3	FM1	a3	Complete Impairment	P	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.
		a4	CCF Impaired	M	The clutch was glazed and too high clearances causing the engine to trip on overspeed.
	FM2	b4	CCF Impaired	M	Fibres probably coming from inappropriate textile absorbent pad used to clean the oil tank, due to a non-precise enough procedure, led to clogged filters of the lubrication system.
			Complete Impairment	M	Fibres probably coming from inappropriate textile absorbent pad used to clean the oil tank, due to a non-precise enough procedure, led to moderately clogged filters of the lubrication system.
			Partial CCF	H	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 .
		b6	Complete CCF	A	Pollution of the air supply due to sandblasting outside the diesel building led to scoring in the sleeves of the cylinders and to high pressure in the motors.
			Complete Impairment	H	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.
		b11	CCF Impaired	H	Confusion between fuel tank "drain valves" of the two diesels, due to operator stress caused by the order of “quick” requalification of the diesel locked for preventive maintenance operation, led to empty the fuel tank of the other diesel.
			Complete CCF	H	Incorrect installation of the service water flow control valves due to procedural inadequacies, inattention to detail and inadequate skills.
			Complete CCF	P	Paint overspray on the DG exciter commutator ring (cause: management deficiency resulting from inadequate work control and management interface).
	FM3	c2	Complete Impairment	D	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.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Partial CCF	I	High resistance of breaker contacts due to hardening of contact lubricant grease. This led to auto-start being inhibited.
		c3	CCF Impaired	D	Failures of tachometers due to broken cables led to the diesel trip.
			Complete CCF	H	Control cable cut off by worker, loss of monitoring.
		c4	CCF Impaired	D	Use of uncalibrated crimpers resulted in deficient crimp connections in EDG wiring connections and failure to start of a EDG.
	FM4	d1	CCF Impaired	H	Due to a coupling of the wrong type, one diesel tripped.
			Complete Impairment	P	Error in the electronic over speed guard due to an incorrect input card to the taco meter.
		d2	CCF Impaired	M	Failure at start-up because of misalignment of low level oil sensors.
		d3	Partial CCF	I	Spurious operation of two diesel generators because of a failed coil of a relay.
		d4	CCF Impaired	D	A wiring error in the EDG control panel lead to a too high increase of diesel power when grid voltage gradually increased during a 24 hours run test.
			CCF Impaired	H	Wrongly re-assembled connector during maintenance leading to that two phases were reversed causing wrong spark sequences from exciter which was not detected because of incomplete testing after maintenance.
			Complete CCF	H	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 two diesels.
			Complete Impairment	D	Increase of the voltage of EDG outside Tech Spec limits due to inadequate wiring of 140 relays.
			Partial CCF	D	The relay wiring configuration related to EDG output breakers had been designed and installed based on an incorrect print.
			Partial CCF	H	Unit trip relays were reset due to operator error preventing EDGs to pick up load when started.
	FM6	f2	No Impairment	M	Impossibility to proceed with full load requalification tests for diesels due to staff, confusing tests and consulting out-of-date documentation.

10. APPENDIX D – Failure analysis matrix – Deficiencies in design, construction and manufacturing

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
D	FM1	a1	Complete Impairment	D	EDG air start system regulator drifted up to pressure outside the nominal operating range. It was determined that these regulators were not optimal for this application due to flow rate considerations.
			Incipient Impairment	D	There was not a failure of the engine to start but the potential was there for a start failure due to the air start solenoid valves not operating consistently below 90 V DC and below 200 psig.
		a2	CCF Impaired	D	Turbocharger damaged due to a piece part that got loose.
			CCF Impaired	D	Failure of fuel pipes due to pressure pulsations. The production process of the fuel pipes was not adequate (no auto-frettage).
			Complete Impairment	D	Fatigue cracks on diesel engine parts (con-rods).
			Complete Impairment	D	Fatigue behaviour of connected rods of both diesels leading to cracks, due to inappropriate design.
			Incipient Impairment	D	Pushrods were broken ore bend beyond specification because of the use of insufficient materials and surface treatment.
			Single Impairment	D	Cracks in two out of 12 con-rods.
		a3	CCF Impaired	I	Two injection pumps got stuck due to two cylinder piston degradation.
			CCF Impaired	M	Failure of fuel booster pump, wrong type of bolt was used. Detected in periodic test.
			Complete Impairment	D	EDG governor instabilities were caused by air trapped in the governor compensation system.
			Complete Impairment	I	A small leak in the cylinder head leading to low starting air pressure.
			Incipient Impairment	D	A liquid penetrant test conducted in the overhaul inspection of EDG A and B revealed flaw indications exceeding the acceptable level in the piston pin.
			Incipient Impairment	I	Leak of fuel injection nozzles for two DGs. Detected in periodic test.

1. FCC = Failure cause category, see Section 4.1
2. FM Cat = Failure mechanism category, see Section 4.1
3. FM Sub = Failure mechanism sub-category, see Section 4.1
4. See Section 3.1 for the definitions of event severities.
5. See Section 3.3 for the acronyms of root causes.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Incipient Impairment	I	Leak of two fuel injection nozzles. Detected in periodic test.
		a4	CCF Impaired	I	Oil and graphite paste from open sump contaminating the diesel clutch leading to failed diesel.
			Complete Impairment	D	Defective potentiometer, DG could not load power controlled.
		a5	Complete CCF	C	Event description too sparse.
			Complete Impairment	A	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.
			Complete Impairment	A	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.
			No Impairment	H	The in- and outlets of the lubrication-piping of the turbocharger were exchanged. This caused the turbocharger to fail due to bad lubrication.
	FM2	b1	CCF Impaired	D	DG failed due loss of cooling caused by ice forming in the service water pump column (environmental conditions).
			CCF Impaired	H	Inadvertent opening of sea water recirculation gates invoked large amounts of sludge movement which blocked the sea water heat exchangers.
			Complete Impairment	D	Crack in connection tube led to bad connection of a test valve on the jacket cooling which could have caused a pipe rupture.
			Complete Impairment	D	Inappropriate materials in combination with salt water caused corroded valves, leading to air in the system and low water pressure.
			Complete Impairment	I	Contamination (mostly iron) led to the measure pipe to clog in the internal cooling water system leading to alarm for low water pressure.
			Incipient Impairment	A	Sludge movement in the sea water channel led to reduced heat capacity of sea water heat exchangers.
			Partial CCF	D	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.
			Partial CCF	H	Erroneous closing of sea water gates invoked large amounts of sludge movement which blocked the sea water heat exchangers.
		b2	CCF Impaired	D	Temperature controller failure due to loop motor blockage led the thermostatic three-way valve to stay on the "cooling bypass" position.
			Complete Impairment	U	Thermostat signal, which controls the cooling system of the diesels, outside the tolerance range.
			Complete Impairment	U	Temperature control channel malfunction led to the potential unavailability of thermostatic three-way-valve.
			Incipient Impairment	A	Change of flow conditions in the sea water channel caused sludge (mussels etc.) unfastening which led to reduced flow through heat exchangers and decreased heat removal capacity.
			Incipient Impairment	A	Sludge movement in the sea water channel led to reduced heat capacity of sea water heat exchangers.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Incipient Impairment	H	Change of flow conditions in the sea water channel caused sludge (mussels etc.) unfastening which led to reduced flow through heat exchangers and decreased heat removal capacity.
		b3	CCF Impaired	D	electrical potential between different materials lead into corrosion and to leaks of the cooling water pipes and failure of diesel generators.
			CCF Impaired	D	Leakage of internal cooling water due to corrosion.
			Complete Impairment	D	Mechanical failure of cooling water jacket resulted in leakage attributed to inadequate vibration tolerant design.
			Complete Impairment	D	Corrosion of sacrificial anode caused it to become loose and the screw holding the anode in place had loosened.
			Complete Impairment	D	Mechanical failure of cooler piping.
			Complete Impairment	U	Leakage of antifreeze from diesel preheating system lead to green sludge in fuel pump mechanical seal and degraded function of diesel.
			Single Impairment	D	Leakage in high temperature cooling circuit caused by engine vibrations.
			Single Impairment	D	Leakage in high temperature cooling circuit caused by engine vibrations.
			Single Impairment	D	Leakage in high temperature cooling circuit caused by engine vibrations.
		b4	CCF Impaired	D	Cool air led to low viscosity of oil in oil pressure measurement line and too slow build-up of oil pressure signal, which caused the component protection to switch off the diesel.
		b5	CCF Impaired	D	Low sump oil temperature due to cold weather and non-functioning sump heater led to excessive run-up times.
		b6	CCF Impaired	D	Vibrations led to the widening of the clearance between limit switch tapped and actuator cam. Diesel was shut off by component protection.
			Complete Impairment	A	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.
			Complete Impairment	D	EDG room air temperatures too high due to recirculation of air.
		b8	CCF Impaired	D	EDGs Fail to Start Due to Loss of Prime fuel oil Booster Pumps caused by air entering the pump at the shaft seal.
			Complete CCF	I	Coupling pins failure led to loss of fuel supply preventing the EDG to start.
			Complete Impairment	D	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply system.
			Complete Impairment	D	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).
			Complete Impairment	D	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply lines.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Complete Impairment	D	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply system.
			Complete Impairment	D	Improper design of supporting clamps causing vibration and abnormal wear of fuel supply pipes around the supporting clamps.
			Complete Impairment	U	Corrosion leads to abnormal wear on fuel supply pipes around the supporting clamps.
			Complete Impairment	U	Corrosion leads to abnormal wear on fuel supply pipes around supporting clamps.
			Partial CCF	I	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.
		b9	Complete Impairment	A	Seized fuel pump probably due to too dry oil and inappropriate storage tanks.
		b10	Complete Impairment	D	Corrosion of fuel pipe supplying all diesel day tanks due to inappropriate pipeline support (design?) leading to not monitored loss of fuel.
			Complete Impairment	D	small leak from the injection tube to cylinder because of a crack.
			Incipient Impairment	D	A small leak was detected in the high-pressure pipe between injection pump and the injector on the diesel.
			Incipient Impairment	D	A small leak was detected in the high-pressure pipe between injection pump and the injector on the diesel.
			Incipient Impairment	D	EDG was found to have fuel oil leak at the fuel injection pump during surveillance test.
		b11	Complete Impairment	D	glycol leak due to thermal and mechanical stresses on a hose could have caused failure of the EDG to run due to fire.
			Incipient Impairment	D	Vibrations due to the running diesels led to cracks in the exhaust gas system.
			Incipient Impairment	D	Vibrations due to the running diesels led to cracks in the exhaust gas system.
	FM3	c2	CCF Impaired	D	Failure to start due to failure of the speed detection circuit. This was a result of poor design of the output connectors and insufficient testing procedures and monitoring to confirm output.
		c3	CCF Impaired	D	Improper design causing bad control cabinet ventilation causing high temperature leading to failed transistor and failed voltage regulator and failure of DG.
			CCF Impaired	D	Vibration caused failure of tachometer.
			CCF Impaired	I	Contactor of tachometer was broken. Failure was identified during test.
			Complete CCF	I	Short circuits in two diodes in the rectifier bridge caused a protective fuse to blow, which resulted in failure of the EDGs to produce the expected voltage.
			Complete Impairment	O	Erratic load control due to intermittent failure of the governor electric control of diesel generator; output breaker opened on a reverse power trip.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
		c4	Complete Impairment	D	Failure of the DG due to voltage regulator failure because of high reactive power.
	FM4	d1	CCF Impaired	D	Parts of the load governor of the diesel were not probably attached to the engine which caused this governor to fail.
			CCF Impaired	I	Loose connection to speed counter leading to no signal that right rpm was achieved, causing error alarm during diesel start-up.
			Complete CCF	D	Misoperation of the digital time sequencer for automatic loading due to inadequate design.
			Complete CCF	D	Design deficiency in the carbon dioxide fire protection system auxiliary circuitry caused a fuse to blow.
		d2	Complete Impairment	P	Vibration of a locking screw caused the temperature guard to trip too early, leading to faulty signal for high temperature.
		d3	CCF Impaired	A	Switching operation of transformers led to electromagnetic interference causing tripped tachometer and overspeed protection of diesels.
			CCF Impaired	D	Water dripping from leaking cylinder head, it disabled electrical control components.
			Incipient Impairment	D	Vibrations loosened the connector of the thermos-couple and caused inadvertent trip on high exhaust gas temperature.
			Single Impairment	D	Unable to start due to an incorrect signal from the fire extinguisher system.
		d4	Partial CCF	H	Modification to 110V dc system led to incorrect fuses being used on the diesel system leading to failure to run.
	FM5	e2	Complete Impairment	H	Pump test procedure leading to wrong position of fuel transfer pump valves leading to not being able to fill day tanks.
		e3	Complete CCF	D	A repair work at the reactor protection system cubicle caused a spurious signal that started the DGs. DGs stopped when the signal disappeared and were unavailable for about 2 minutes.
	FM6	f2	Complete Impairment	D	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.
C/M	FM1	a1	CCF Impaired	D	DG fail to start due to air valve pistons sticking because of inadequate manufacturing tolerances.
			CCF Impaired	D	inadequate manufacturing tolerances resulted in sticking of air valve pistons.
			CCF Impaired	I	Wrong material of bolts led to fatigue which caused the pin bolts to the start air valve to crack and become loose.
			Complete Impairment	I	Design of diesel air manifold led to cracking in operation/over time.
		a2	CCF Impaired	D	Magnetic pickup target gear shaft failed during load test. A manufacturer defect in the shaft caused the failure. The same component was installed on other diesels at the site.
			CCF Impaired	D	Alarm for high crankcase pressure caused the engine to shut down.
			CCF Impaired	D	Incorrect manufacture process (balancing first and welding after) leading to unbalanced turbo-charge causing vibrations and failure of the rotor.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Incipient Impairment	D	Magnetic pickup target gear shaft failed during load test. A manufacturer defect in the shaft caused the failure. The same component was installed on other diesels at the site.
		a3	CCF Impaired	I	Damaged pistons, sleeves and packing rings due to inappropriate manufacturing process of pistons and inadequate cladding of packing rings.
			CCF Impaired	I	cylinder injection pump broke because of screws rupture due to improper pump fixing.
			Complete Impairment	I	Injection pump breakage due to three screws rupture on the pump cover caused by improper fixing on the EDG casing and by vibrations generated during the EDG running.
			Incipient Impairment	D	Cracked fuel injector nozzle tips found in EDGs caused by manufacturing error.
		a4	CCF Impaired	I	Elastic coupling between generator and diesel motor broke. Durability (life time) shorter than specified by supplier.
		a5	Complete Impairment	D	Multiple valve adjustment assemblies cracked due to manufacturing defect.
	FM2	b2	CCF Impaired	D	Improper installation of the rod/drive shaft on the three-way valves led to loss of cooling, which would have led to both EDG unavailabilities.
		b3	Complete Impairment	D	External corrosion due to rainwater accumulation of the EDG cooling pipes led to leak.
			Complete Impairment	D	Slight leaks on cooling pipes due to rainwater penetration in the EDG building which had been accumulated between the cooling pipes and the insulating sleeves.
			Complete Impairment	D	External corrosion on cooling pipes due to penetration of rain water because of a non-leak-proof EDG building.
			Complete Impairment	D	Rain water penetration to the EDG building led to external corrosion, which caused slight leaks on cooling pipes.
		b5	CCF Impaired	D	Too low sump oil temperature due to incorrect electrical supply to oil heaters.
		b6	CCF Impaired	D	Crack is found in the exhaust damper linkage roll pin due to inadequate design.
			CCF Impaired	D	Due to air in the fuel line, the FY 61 diesel generator failed to start. After venting of the fuel line, the diesel started properly.
	FM3	c2	CCF Impaired	D	Weak return springs in the exciter trip switch caused the switch to fail.
			CCF Impaired	I	Generator output breaker tripped, which led to failure to synchronise the generator with safety bus.
			CCF Impaired	I	Random failure of monitoring equipment, block DG to start if demanded.
			Complete CCF	D	Lockout relay of both EDG output breakers were found sticking (not tripping when required).
	FM4	d1	CCF Impaired	I	Both EDGs failed to start due to failure of the same relay subcomponent. One relay had high contact resistance while the other relay was found to have missing parts. The shared cause factor is low.
			CCF Impaired	I	A wire wound potentiometer showed high contact resistance which resulted in triggered overspeed guard.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
D-MOD	FM1	a5	Complete CCF	D	A design modification in the turbocharger of EDGs resulted in resonance vibrations during operation and failures of fan blades.
			Complete Impairment	D	The turbo of diesel generator units were replaced. Misjudgement of the new turbo wall inserts lead to an unanticipated resonance induced vibration resulting in fatigue failure of compressors impeller blade.
	FM2	b2	CCF Impaired	D	Thermostatic three-way valve malfunction due to probably scrubbing of valve internal pieces.
			CCF Impaired	D	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.
			CCF Impaired	D	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.
			CCF Impaired	D	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.
			CCF Impaired	I	Anti-rotation pin failure led to gap between the rod/valve assembly, probably caused by non-evolving “metallic fold” defect appeared during the “hot forged” manufacturing, led to thermostatic three-way-valve failure.
			Complete Impairment	D	Thermostatic three-way-valve incipient failure due to valve/rod anti-rotation pin failure but without valve/rod assembly unscrewing.
			Complete Impairment	D	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel.
			Complete Impairment	D	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel.
	FM3	c2	CCF Impaired	D	Exciter switch failure due to an unsuitable spring. The spring hat been retrofitted following a recommendation by the manufacturer which was issued after a licensee event report. The spring was unsuitable because the manufacturer had not considered a design change of the s.
		c3	CCF Impaired	D	Circuit breaker failure due to early ageing of a contactor due to voltage change from 220 to 230 V (beyond design).
	FM4	d2	Partial CCF	C	Error when changing the instrumentation led to overestimation of the diesel fuel tank level.
	FM5	e2	Complete Impairment	D	Diesel generator not able to reach design load due to misadjusted engine governor output linkage.

11. APPENDIX E – Specific events

E.1 Complete CCF

Complete CCF events are identified in the "Event severity" columns in Appendix C and D.

E.2 CCF outside planned test

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM2	b8	CCF Impaired	H	Due to difficulties in reading the dipstick when the diesel is running it was not discovered that the oil level was low and hence the diesel generator stopped.
			CCF Impaired	P	EDG fuel oil transfer pump when day tank level was below start set point due to a failed low level cut-out switch. The second EDG fuel oil transfer pump failed due to a blown control power fuse making both EDGs unavailable for auto-start.
O3	FM4	d4	Partial CCF	H	Unit trip relays were reset due to operator error preventing EDGs to pick up load when started.
D	FM2	b6	Complete Impairment	A	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.
		b8	Complete Impairment	D	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply system.
			Complete Impairment	D	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply lines.
			Complete Impairment	D	Inappropriate supporting clamp design + vibrations during running EDG causing cracks in fuel supply system.
			Partial CCF	I	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.
		b10	Complete Impairment	D	Corrosion of fuel pipe supplying all diesel day tanks due to inappropriate pipeline support (design?) leading to not monitored loss of fuel.
	FM4	d3	CCF Impaired	D	Water dripping from leaking cylinder head, it disabled electrical control components.
		d4	Partial CCF	H	Modification to 110V dc system led to incorrect fuses being used on the diesel system leading to failure to run.
	FM5	e2	Complete Impairment	H	Pump test procedure leading to wrong position of fuel transfer pump valves leading to not being able to fill day tanks.

E.3 Component not capable

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM2	b1	Partial CCF	H	Valve for cooling water not opened again after repair causing high water temperature
		b11	CCF Impaired	H	improper greasing of fuel oil pump motor bearings rendered pumps inoperable during extremely cold weather conditions
O3	FM2	b6	Complete Impairment	H	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
D	FM1	a4	Complete Impairment	D	Defective potentiometer, DG could not load power controlled
	FM2	b1	Partial CCF	D	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
	FM3	c3	CCF Impaired	D	Improper design causing bad control cabinet ventilation causing high temperature leading to failed transistor and failed voltage regulator and failure of DG
	FM6	f2	Complete Impairment	D	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
D-MOD	FM2	b2	Complete Impairment	D	Thermostatic three-way-valve incipient failure due to valve/rod anti-rotation pin failure but without valve/rod assembly unscrewing
	FM3	c3	CCF Impaired	D	Circuit breaker failure due to early ageing of a contactor due to voltage change from 220 to 230 V (beyond design)

E.4 Multiple defences failed

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM6	f2	Complete CCF	H	Complex procedure overloaded by handwritten remarks led to reconnect a diesel without complete requalification test and to erroneously disconnect a diesel on another unit
D	FM3	c3	CCF Impaired	D	Improper design causing bad control cabinet ventilation causing high temperature leading to failed transistor and failed voltage regulator and failure of DG

E.5 New failure mechanism

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM2	b9	CCF Impaired	P	Loss of lubrication capacity of the fuel injection pump of DG due to the use of inadequate diesel fuel (low sulphur)
	FM6	f1	CCF Impaired	A	Over temperature 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.
D	FM1	a4	CCF Impaired	I	Oil and graphite paste from open sump contaminating the diesel clutch leading to failed diesel
		a5	Complete Impairment	A	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.
			Complete Impairment	A	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.
	FM2	b1	CCF Impaired	H	Inadvertent opening of sea water recirculation gates invoked large amounts of sludge movement which blocked the sea water heat exchangers
			Incipient Impairment	A	Sludge movement in the sea water channel led to reduced heat capacity of sea water heat exchangers.
			Partial CCF	H	Erroneous closing of sea water gates invoked large amounts of sludge movement which blocked the sea water heat exchangers
		b5	CCF Impaired	D	Low sump oil temperature due to cold weather and non-functioning sump heater led to excessive run-up times
		b6	Complete Impairment	A	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.
		b8	Complete CCF	I	Coupling pins failure led to loss of fuel supply preventing the EDG to start
		b11	Complete Impairment	D	glycol leak due to thermal and mechanical stresses on a hose could have caused failure of the EDG to run due to fire
	FM4	d3	CCF Impaired	A	Switching operation of transformers led to electromagnetic interference causing tripped tachometer and overspeed protection of diesels
D-MOD	FM1	a5	Complete Impairment	D	The turbo of diesel generator units were replaced. Misjudgement of the new turbo wall inserts lead to an unanticipated resonance induced vibration resulting in fatigue failure of compressors impeller blade.

E.6 CCF sequence of different CCF

No events.

E.7 CCF cause modification

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM5	e2	CCF Impaired	H	EDGs observed in underspeed condition due to inadequate maintenance on governor replacement and adjustment and inadequate post-maintenance testing.
	FM6	f2	Complete CCF	P	Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply.
			Complete Impairment	P	Locking of automatic start-up of both EDGs were erroneously required by the test procedure on another component.
O3	FM2	b6	Complete CCF	A	Pollution of the air supply due to sandblasting outside the diesel building led to scoring in the sleeves of the cylinders and to high pressure in the motors.
	FM4	d4	Partial CCF	D	The relay wiring configuration related to EDG output breakers had been designed and installed based on an incorrect print.
D	FM1	a5	Complete Impairment	A	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.
			Complete Impairment	A	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.
	FM2	b3	CCF Impaired	D	electrical potential between different materials lead into corrosion and to leaks of the cooling water pipes and failure of diesel generators.
			Complete Impairment	D	Mechanical failure of cooling water jacket resulted in leakage attributed to inadequate vibration tolerant design.
	FM4	d1	Complete CCF	D	Misoperation of the digital time sequencer for automatic loading due to inadequate design.
	FM6	f2	Complete Impairment	D	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.
C/M	FM1	a1	CCF Impaired	D	DG fail to start due to air valve pistons sticking because of inadequate manufacturing tolerances.
	FM2	b3	Complete Impairment	D	External corrosion due to rainwater accumulation of the EDG cooling pipes led to leak.
D-MOD	FM2	b2	CCF Impaired	D	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.
			CCF Impaired	D	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.
			CCF Impaired	I	Anti-rotation pin failure led to gap between the rod/valve assembly, probably caused by non-evolving “metallic fold” defect appeared during the “hot forged” manufacturing, led to thermostatic three-way-valve failure.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Complete Impairment	D	Thermostatic three-way-valve incipient failure due to valve/rod anti-rotation pin failure but without valve/rod assembly unscrewing.
			Complete Impairment	D	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel.
			Complete Impairment	D	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel.

E.8 Multiple systems affected

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM4	d2	Single Impairment	D	Misadjusted settings of the fuel amount governor led to fluctuations of the rotation speed in the start-up process and thereby to the shut-off of the diesel.[1]
D	FM1	a2	CCF Impaired	D	Turbocharger damaged due to a piece part that got loose.[1]

E.9 Common-Cause Initiator

No events.

1. The plants where these events occurred have two different types of EDGs which are modelled in two different common cause component groups. The observed failure mechanism was present at both types of EDGs, so the events are assessed as "Multiple systems affected".

E.10 Safety culture

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM1	a3	Complete Impairment	P	Sandblast cleaning of the combustion air intercoolers caused sand to be introduced into the engines and then scoring of cylinder liners and piston rings
	FM2	b8	Complete Impairment	D	Inaccurate level instrumentation + human error (not responding to alarm) causing too small fuel level margin without knowing
		b10	CCF Impaired	M	Re-using of piece part that needs to be replaced during maintenance led to fuel leakage. (Root cause unknown: maintenance documentation or execution?)
	FM4	d4	Partial CCF	H	Low voltage due to insufficient torqued screw in a connection block prevented start of DG
	FM5	e2	Complete CCF	H	Diesels were taken out of service which was against the station operation procedure
	FM6	f2	Complete CCF	H	Complex procedure overloaded by handwritten remarks led to reconnect a diesel without complete requalification test and to erroneously disconnect a diesel on another unit
			Complete CCF	P	Test procedure which erroneously required locking of automatic start-up of both EDGs was not corrected due to a lack of monitoring in procedure modifications
O3	FM4	d4	CCF Impaired	H	Wrongly re-assembled connector during maintenance leading to that two phases were reversed causing wrong spark sequences from exciter which was not detected because of incomplete testing after maintenance

E.11 Multi-unit CCF

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
O1	FM1	a3	Complete Impairment	P	Sandblast cleaning of the combustion air intercoolers caused sand to be introduced into the engines and then scoring of cylinder liners and piston rings.
	FM2	b2	Complete Impairment	A	Tube sheet blockage (primarily corrosion nodules) found in the EDG (environmental issue).
			Complete Impairment	P	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).
			Complete Impairment	P	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).
			Complete Impairment	P	The rod lock-nut was unscrewing which led to incorrect stroke of the three-way valve in the engine water cooling system.
		b8	Complete Impairment	M	wrong calibration of fuel storage tank level could have led to unavailability of the DGs.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
		b11	CCF Impaired	H	Improper greasing of fuel oil pump motor bearings rendered pumps inoperable during extremely cold weather conditions.
	FM3	c2	Complete CCF	A	Cracks in numerous relay sockets were induced by vibrations in the EDG rooms resulting failure of diesel load control.
			Complete Impairment	A	Cracks in numerous relay sockets were induced by vibrations in the EDG rooms could result in failure of diesel load control.
	FM6	f2	Complete CCF	P	Error in the test procedure led to not allowing automatic start of EDG during tests of turbine driven emergency power supply.
			Complete CCF	P	Test procedure which erroneously required locking of automatic start-up of both EDGs was not corrected due to a lack of monitoring in procedure modifications.
			Complete Impairment	P	Locking of automatic start-up of both EDGs were erroneously required by the test procedure on another component.
O2	FM3	c3	CCF Impaired	A	Failure of DG is due to failed resistor in the governor unit due to long term heat fatigue.
			CCF Impaired	A	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.
O3	FM2	b4	CCF Impaired	M	Fibres probably coming from inappropriate textile absorbent pad used to clean the oil tank, due to a non-precise enough procedure, led to clogged filters of the lubrication system.
			Complete Impairment	M	Fibres probably coming from inappropriate textile absorbent pad used to clean the oil tank, due to a non-precise enough procedure, led to moderately clogged filters of the lubrication system.
	FM4	d4	CCF Impaired	D	A wiring error in the EDG control panel lead to a too high increase of diesel power when grid voltage gradually increased during a 24 hours run test.
			Complete Impairment	D	Increase of the voltage of EDG outside Tech Spec limits due to inadequate wiring of 140 relays.
D	FM1	a2	Complete Impairment	D	Fatigue cracks on diesel engine parts (con-rods).
			Single Impairment	D	Cracks in two out of 12 con-rods.
		a5	Complete Impairment	A	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.
			Complete Impairment	A	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.
	FM2	b1	CCF Impaired	H	Inadvertent opening of sea water recirculation gates invoked large amounts of sludge movement which blocked the sea water heat exchangers.
			Incipient Impairment	A	Sludge movement in the sea water channel led to reduced heat capacity of sea water heat exchangers.
		b2	CCF Impaired	D	Temperature controller failure due to loop motor blockage led the thermostatic three-way valve to stay on the "cooling bypass" position.
			Incipient Impairment	A	Change of flow conditions in the sea water channel caused sludge (mussels etc.) unfastening which led to reduced flow through heat exchangers and decreased heat removal capacity.

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Incipient Impairment	A	Sludge movement in the sea water channel led to reduced heat capacity of sea water heat exchangers.
		b8	Complete CCF	I	Coupling pins failure led to loss of fuel supply preventing the EDG to start.
			Complete Impairment	U	Corrosion leads to abnormal wear on fuel supply pipes around the supporting clamps.
			Complete Impairment	U	Corrosion leads to abnormal wear on fuel supply pipes around supporting clamps.
		b11	Complete Impairment	D	Glycol leak due to thermal and mechanical stresses on a hose could have caused failure of the EDG to run due to fire.
	FM4	d3	Incipient Impairment	D	Vibrations loosened the connector of the thermos-couple and caused inadvertent trip on high exhaust gas temperature.
C/M	FM1	a1	CCF Impaired	D	DG fail to start due to air valve pistons sticking because of inadequate manufacturing tolerances.
			CCF Impaired	D	Inadequate manufacturing tolerances resulted in sticking of air valve pistons.
		a2	CCF Impaired	D	Magnetic pickup target gear shaft failed during load test. A manufacturer defect in the shaft caused the failure. The same component was installed on other diesels at the site.
			Incipient Impairment	D	Magnetic pickup target gear shaft failed during load test. A manufacturer defect in the shaft caused the failure. The same component was installed on other diesels at the site.
		a3	CCF Impaired	I	Cylinder injection pump broke because of screws rupture due to improper pump fixing.
			Complete Impairment	I	Injection pump breakage due to three screws rupture on the pump cover caused by improper fixing on the EDG casing and by vibrations generated during the EDG running.
	FM2	b3	Complete Impairment	D	External corrosion due to rainwater accumulation of the EDG cooling pipes led to leak.
			Complete Impairment	D	Slight leaks on cooling pipes due to rainwater penetration in the EDG building which had been accumulated between the cooling pipes and the insulating sleeves.
			Complete Impairment	D	External corrosion on cooling pipes due to penetration of rain water because of a non-leak-proof EDG building.
D-MOD	FM1	a5	Complete CCF	D	A design modification in the turbocharger of EDGs resulted in resonance vibrations during operation and failures of fan blades.
			Complete Impairment	D	The turbo of diesel generator units were replaced. Misjudgement of the new turbo wall inserts lead to an unanticipated resonance induced vibration resulting in fatigue failure of compressors impeller blade.
	FM2	b2	CCF Impaired	D	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.
			CCF Impaired	D	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.
			CCF Impaired	D	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.
			CCF Impaired	I	Anti-rotation pin failure led to gap between the rod/valve assembly, probably caused by non-evolving “metallic fold” defect appeared during the “hot forged” manufacturing, led to thermostatic three-way-valve failure

FCC[1]	FM Cat[2]	FM Sub[3]	Event severity[4]	Root cause[5]	Failure mechanism description
			Complete Impairment	D	Thermostatic three-way-valve incipient failure due to valve/rod anti-rotation pin failure but without valve/rod assembly unscrewing
			Complete Impairment	D	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel
			Complete Impairment	D	Improper design (gap rod/valve) in three-way-valve which controls the cooling system to the diesel