ICDE PROJECT COLLECTION AND ANALYSIS OF COMMON-CAUSE FAILURES OF EMERGENCY DIESEL GENERATORS

Jeffery Wood[1], Anna Georgiadis[2], Mattias Håkansson[3], Gunnar Johanson[4], Albert Kreuser[5]

[1] *United States Nuclear Regulatory Commission, Washington, DC, United States, Jeffery.Wood@nrc.gov*
[2] *ÅF Nuclear Technology, Stockholm, Sweden, anna.georgiadis@afconsult.com*
[3] *ÅF Nuclear Technology, Stockholm, Sweden, mattias.hakansson@afconsult.com*
[4] *ÅF Nuclear Technology, Stockholm, Sweden, gunnar.johanson@afconsult.com*
[5] *Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Cologne, Germany, Albert.Kreuser@grs.de*

The participating countries of the International Common-Cause Failure Data Exchange (ICDE) project have been collecting emergency diesel generator (EDG) common-cause failure (CCF) data since the project's inception in 1994. In May 2000, the ICDE project published a report summarizing the collection and analysis of EDG CCF events. The report examined 106 collected events. Since that time, the ICDE project has continued collection of EDG CCF events. The database now includes 224 EDG CCF events spanning a period from 1977 through 2012. The ICDE project is currently preparing an updated report on EDG CCF events. The objectives of the report are to: describe the EDG data collected by ICDE, develop qualitative insights from the reported events, and describe the failure mechanisms and phenomena involved in the events. This paper gives an overview summary of the 224 EDG CCF events collected by the ICDE project and presents the preliminary insights gained from the analysis of the data.

I. INTRODUCTION

This report presents an overview of the exchange of common-cause failure (CCF) data of emergency diesel generators (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; and
- To develop the failure mechanisms and phenomena involved in the events, their relationship to the root causes, and possibilities for improvement.

Section II presents a description of the emergency diesel generator component. Section III presents an overview of the contents of the EDG database and a summary of statistics. Section IV contains some high level engineering insights about the diesel CCF events. These insights are based on failure causes and failure mechanisms. Section V provides a summary and conclusions.

A brief description of the international common-cause data exchange (ICDE) project, its objectives, and the participating countries, is given below. The preparation for the ICDE project was initiated in August of 1994. Since April 1998 the OECD/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 2018. Member countries under the current Agreement of OECD/NEA and the organizations representing them in the project are: Canada (CNSC), Czech Republic (UJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), Korea (KAERI), Spain (CSN), Sweden (SSM), Switzerland (ENSI), and United States (NRC).

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

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.

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].

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

II. COMPONENT DESCRIPTION

This section is extracted from Emergency Diesel Generator coding guidelines which is an appendix to the general coding guidelines.[1]

II.A. General Description of the Component

Emergency diesels drive generators that are part of the electrical power distribution system providing emergency power in the event of a loss of offsite power to electrical buses that supply the safety systems of the reactor plant. At some plants, emergency diesels also directly drive safety injection pumps and/or emergency feedwater pumps. The EDGs normally are not in service when the plant is operating at power or shutdown.

The systems for which emergency diesel generator (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)

II.B. Component Boundaries

The component 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 EDG are the circuit breakers, which are located at the motor control centers (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 or control logic and the attendant process detectors for system initiations, trips, and operational control.

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

II.C. Event Boundary

The mission for the EDGs is to 1) start and supply motive force/electrical power in the event of a loss of offsite power 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 EDG to start or supply motive force/electrical power in the event of loss of coolant or loss of offsite power.

III. OVERVIEW OF DATABASE CONTENT

This section presents a summary of the data collected for this report.

III.A. Overview

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

The types of nuclear power plants represented in this data collection include: pressurized water reactors, boiling water reactors, Magnox and advanced gas reactors. The data collection include 244 units and 4850 group observation years. Figure 1 presents the data collection of group observation times (years) and number of events distributed over time.

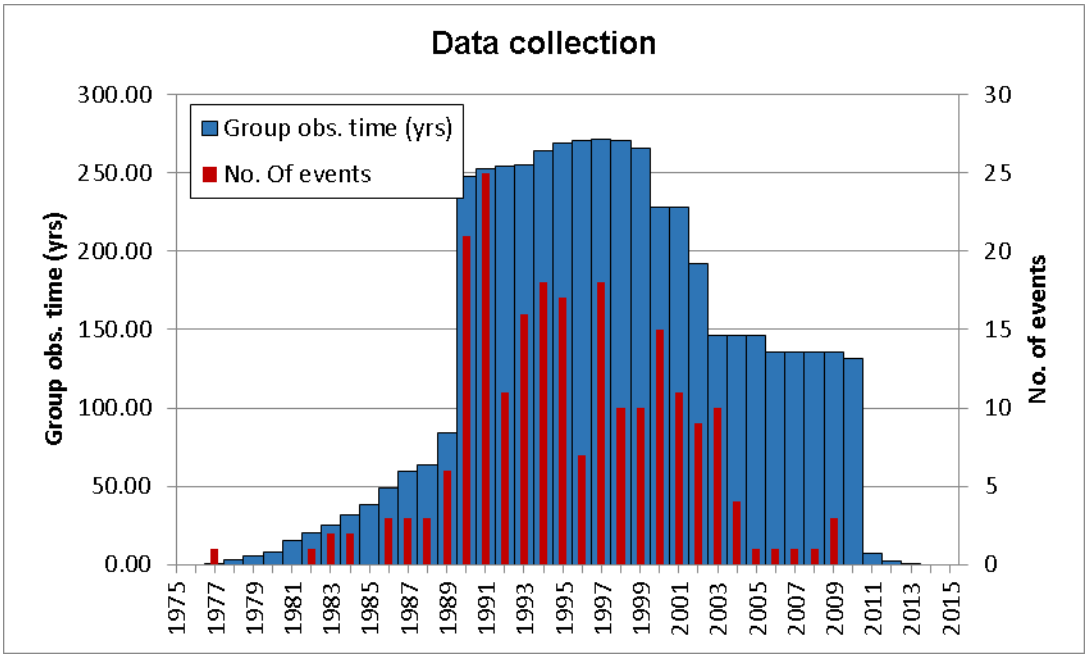

Figure 1. Data collection: Observation time and event count distributed over time

Collecting these events have included both top-down work by identifying events on 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 sections are strictly based on the coding scheme given in the ICDE coding guidelines.[1] The following sections present a deeper engineering analysis of the events.

III.B. Failure mode and Impact of Failure

For each event in the ICDE database, the impairment of each component in the observed population has been defined according to the categorisation of the general coding guidelines.[1] The interpretation of impairment categories for emergency diesel generator are 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 1 shows the distribution of the events by failure mode and severity degree. The most dominant severity categories are not the most severe, categories c) "CCF impaired" and d) "Complete impairment", which indicates the need to assess all levels of severity in CCF analyses. 23 of the events (10%) were complete CCF events. The most common failure mode is "failure to run" (62%), followed by "failure to start" (37%).

TABLE 1. Distribution of Severity per Failure Mode

Failure mode	No. of events	Severity category (See note * for category definitions.)						
		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**	**16**	**89**	**66**	**21**	**6**	**3**

III.C. 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

* *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 impariment = All components working.

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 2 shows the distribution of the events by root causes. 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. 51% of the events with root cause coded as D involve failures of ancillary systems. After ancillary systems, the next highest contribution of design errors involve 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 twelve different reactor units.

TABLE 2. Distribution of Root Cause per Severity Category

		Severity category						
	No. of events	**a**	**b**	**c**	**d**	**e**	**f**	**g**
Abnormal environmental stress (A)	19	4	1	5	6	3		
State of other components (C)	3	1	1			1		
Design, manufacture or construction inadequacy (D)	98	5	2	38	35	11	6	1
Human actions (H)	25	6	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**

III.D. 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 shows 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. Distribution of Coupling Factors per Severity Category

		Severity 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**

III.E. 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 4 contains 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. The low number of demand events suggests that diesel failures may be easier to detect in periodic tests compared to other type of failures or failures in other components.

TABLE 4. Distribution of Detection Methods per Severity Category

	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**

III.F. 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 program 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 5. Twenty-five percent of the corrective actions are made by “Design modifications” (C), followed by “Specific maintenance/operations practices” (A).

TABLE 5. Distribution of Corrective Actions per Severity Category.

	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 component (G)	32	3	3	11	9	4	1	1
Other (O)	15	1	2	4	6	2		
empty	7			2	5			
Total	**224**	**23**	**16**	**89**	**66**	**21**	**6**	**3**

IV. ENGINEERING ASPECTS OF THE COLLECTED EVENTS

This section contains an engineering review of the diesel events to assist in drawing useful conclusions from the data. This process is performed collectively by the ICDE participants working together in small groups.

IV.A. Assessment Basis

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 currently applied failure analysis areas are summarized in the ICDE Failure Analysis Coding Guide (project internal document), which aims at supporting the analyst during the review. The failure analysis in this report is based on the following definitions extracted from:

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.

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 T, the six failure mechanism categories and their sub-categories for emergency diesel events are presented.

TABLE 6. 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 ancilliary 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

Failure mechanism category and sub-category	
Deficient control and deficient protective cut-out (I&C problems) (FM4)	
d1	Defective or unsuited piece part
d2	Misadjusted setpoints
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 type 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 aging 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 events 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.

IV.B. Failure analysis assessment matrix

In Table 7 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 IV.A are assigned to the columns of the matrix, the failure cause categories as defined in section IV.A 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 ancilliary systems (45% of events), followed by engine damage or problems (26%), I&C problems (13%), and electrical failures (12%). The ancilliary 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 are 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%).

TABLE 7. Failure Analysis Assessment Matrix

Failure cause category	**Failure mechanism category**						
	Engine damage or problems	**Compro-mised ancilliary 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**

IV.C. Failure Analysis Assessment of Deficiencies in Operation

In Table 7, 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.

O1 Deficient procedures for maintenance and/or testing:

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.

O2 Insufficient attention to aging of piece parts:

Failure cause O2, insufficient attention to aging 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 aging management program.

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

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 programs and appropriate work controls.

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 instrumentation and control 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.

IV.D. Failure Analysis Assessment of Deficiencies in Design, Construction and Manufacturing

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.
- Cracks found in fuel injector nozzles due to inadequate design and manufacturing.

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.

IV.E. 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 8 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. 26 of the 39 severe events (67%) are caused by deficiencies in operations. Considering the distribution of failure mechanisms, the highest contribution category is compromised ancilliary systems (41%) followed by I&C problems (26%). There are only 28 total events that involved I&C failures (as shown in Table 7), and 10 of these are high severity categories. So, 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.

IV.F. Other Interesting Events

In Table 9 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.

TABLE 8. Failure Analysis Assessment Matrix for Complete and Partial CCF Events

	Failure Mechanism Categories						
Failure Cause Categories	**Engine damage or problems**	**Compro-mised ancilliary systems**	**Electrical failures**	**Deficient control or deficient protective cut-out (I&C problems)**	**Misalign-ment**	**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, manufactur-ing	**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 9. Applied Interesting Event Codes

Interesting CCF event code	**Description**	**No. of events**	**Percent**
1 - CCF Complete	Complete failure of all components	22	10%
2 - CCF Outside planned test	The event was detected outside of normal periodic and planned testing and inspections	12	5%
3 - CCF Component not-capable	Two or more components were not capable to perform its safety function over a long period of time	9	4%
4 - CCF Multiple defences failed	Two or more defence in depth levels were affected	2	1%
5 - CCF New failure mechanism	Unattended or not foreseen failure mechanism	14	6%
6 - CCF Sequence of different CCF	Sequence of different CCF failures and/or subtle dependencies	0	0%
7 - CCF Causes modification	Event causes major modification, e.g. exchange of diesel	19	8%
8 - CCF Intersystem dependency	Event affecting two or more different systems or functions	2	1%
9 - CCF IE_CCI	Event which is both a CCF event and a initiating event causing loss of needed safety system	2	1%
10 – Safety culture	Reason of event originates from major deficiencies in safety culture management	9	4%

Interesting CCF event code	Description	No. of events	Percent
11 – CCF Multiple units	Failure mechanism appeared in a fleet of reactors or multiple units at one site	50	22%
12 – No mark applicable	Indicates that event has been analysed but none of the above marks is applicable	98	44%
Total no. applied codes		**239**	**-**

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

- New common-cause failure 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 overspeed 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.
- 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 loss of offsite power 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 III.C. 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 prioritizing 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.

V. SUMMARY AND CONCLUSIONS

Organizations from Canada, Finland, France, Germany, Japan, Korea, Spain, Sweden, United Kingdom and United States contributed CCF data of Emergency Diesel Generators to this data exchange. 229 ICDE events were reported from nuclear power plants in these countries. These reported ICDE events were reviewed in sections III and IV of this report with respect to degree of failure, failure causes and failure mechanism. A number of notable conclusions can be drawn from this data review. The following notable observations are made.

The most frequently occurring causes of emergency diesel generator failures are design errors related to design, manufacture or construction inadequacy (root cause category D) with 44% of the events. Many of the events involve design issues with piece parts or sub-systems.

The most common type of diesel generator failure mechanism is comprised ancillary systems with 44% 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 (25% of events), I&C problems (13%), and electrical failures (12%).

10% 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.

50 diesel generator CCF events have been marked as impacting multiple reactor units.

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.

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.

ACKNOWLEDGMENTS

The following people 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 people with whom they liaise in all participating countries are recognized as important contributors to the success of this study. Axel Breest has been the administrative NEA officer and has supported the preparation of the report.

REFERENCES

1. International Common-Cause Failure Data Exchange, *ICDE General Coding Guidelines ICDE CG00*, CSNI Tech Note publication NEA/CSNI/R(2004)4. Rev. 2, October 2005.
2. International Common-Cause Failure Data Exchange, *Collection and Analysis of Common-cause Failure of Emergency Diesel Generators*, [NEA/CSNI/R(2000)20], May 2000.