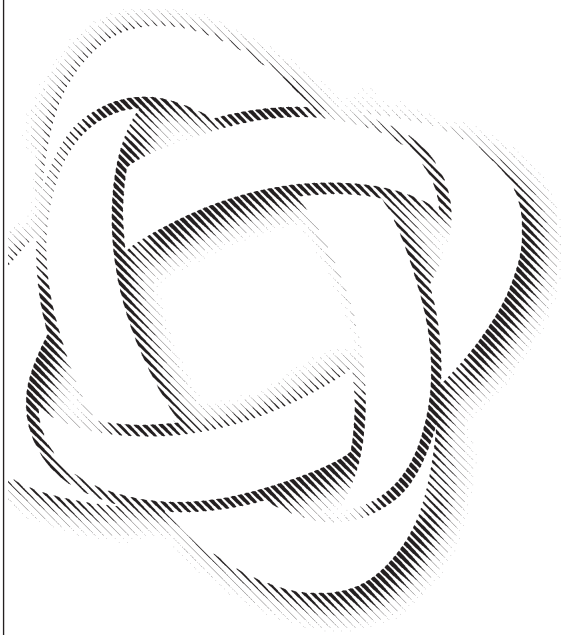
Nuclear Safety
NEA/CSNI/R(2008)1
January 2008

ICDE Project Report : Collection and Analysis of Common-cause Failures of Switching Devices and Circuit Breakers

October 2007



OECD Nuclear Energy Agency
Le Seine Saint-Germain - 12, boulevard des Îles
F-92130 Issy-les-Moulineaux, France
Tél. +33 (0)1 45 24 82 00 - Fax +33 (0)1 45 24 11 10
Internet: http://www.nea.fr

N U C L E A R • E N E R G Y • A G E N C Y

Unclassified **NEA/CSNI/R(2008)1**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **25-Jan-2008**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2008)1
Unclassified

ICDE Project Report: Collection and Analysis of Common-Cause Failures of Switching Devices and Circuit Breakers

October 2007

JT03239279

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 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, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities 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.

* * *

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities 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 friendly and economical use of nuclear energy for peaceful purposes, as well as
- 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 policy analyses in areas such as energy and sustainable development.

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

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of senior scientists and engineers, with broad responsibilities for safety technology and research programmes, and representatives from regulatory authorities. It was set up in 1973 to develop and co-ordinate the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations.

The committee's purpose is to foster international co-operation in nuclear safety amongst the OECD member countries. The CSNI's main tasks are to exchange technical information and to promote collaboration between research, development, engineering and regulatory organisations; to review operating experience and the state of knowledge on selected topics of nuclear safety technology and safety assessment; to initiate and conduct programmes to overcome discrepancies, develop improvements and research consensus on technical issues; to promote the coordination of work that serve maintaining competence in the nuclear safety matters, including the establishment of joint undertakings.

The committee shall focus primarily on existing power reactors and other nuclear installations; it shall also consider the safety implications of scientific and technical developments of new reactor designs.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA) responsible for the program of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH), NEA's Radioactive Waste Management Committee (RWMC) and NEA's Nuclear Science Committee (NSC) on matters of common interest.

PREFACE

The purpose of the International Common Cause Data Exchange (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:

a) Collect and analyse Common-Cause Failure (CCF) events over the long term so as to better understand such events, their causes, and their prevention;

b) 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;

c) Establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defenses against their occurrence, such as indicators for risk based inspections;

d) Generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries; and

e) 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 openly. It is not the aim of those reports to provide direct access to the CCF raw data recorded in the ICDE databank. The confidentiality of the data is a prerequisite of operating the project. The ICDE database is accessible only to those members of the ICDE Project Working Group who have actually contributed data to the databank.

Database requirements are specified by the members of the ICDE Steering Group and are fixed in the ICDE coding guidelines. It is assumed that the data will be used by the members, e.g., in the context of PSA/PRA reviews and application.

ACKNOWLEDGEMENTS

The following people have significantly contributed to the preparation of this report by their personal effort: Begoña Pereira (Empresarios Agrupados), Mª Rosa Morales (CSN), Rafael Cid (CSN), Wolfgang Werner (SAC), Albert Kreuser (GRS), Dale Rasmuson (USNRC), and Gunnar Johanson (ES-konsult). In addition, the ICDE Steering Group and the people with whom they liaise in all participating countries are recognized as important contributors to the success of this study. Pekka Pyy has been the administrative NEA officer and contributed to finalising the report.

TABLE OF CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

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, CSNI formally approved the carrying out of this project within the OECD NEA framework. The project has successfully operated over four consecutive terms (the current term being 2005-2008). The fifth term has been planned to begin in April 2008.

The objectives of the ICDE are to a) collect and analyse CCF events over the long term so as to better understand such events, their causes, and their prevention; b) to 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; c) to 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; d) to generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries; and e) to use the ICDE data to estimate CCF parameters. The ICDE Project aims to include all possible events of interest, comprising complete, partial, and incipient CCF events, called “ICDE events”. The ICDE events are defined as “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.”

The ICDE Project has furthermore established a principle that it shares the engineering insights of its analyses through the NEA Committee on Safety of Nuclear Installations (CSNI) by writing public reports of the analysis results of each component.

This report documents a study performed on a set of ICDE events related to switching devices and circuits breakers (CBs). The events studied here had been collected in the ICDE database. Organizations from Canada, Finland, France, Germany, Spain, Sweden, United Kingdom and United States contributed to the exchange. The ICDE Project is the only international effort where large amounts of data from different countries are collected and analysed to draw conclusions about common cause failures.

One-hundred-four (104) ICDE events, exhibiting at least some degree of dependency, and spanning a period from 1983 through 2004, were examined in the study. The data are not necessarily complete for each country through this period. The available information on the events is limited sometimes depending on the detail of description in licensee event reports or plant maintenance sheets. The database contains general statistical information about event attributes like impairment of the components in the observed populations, root cause, coupling factor, detection methods and corrective actions taken. The events contained in the ICDE database were analysed with respect to failure modes, degree of impairment, failure symptoms, failure causes, and technical fault aspects.

Three **failure modes** were specified for CBs in the ICDE coding guidelines: “failure to open”, “failure to close,” and “spurious operation.” The most frequently encountered failure mode of CBs was "failure to close," representing 42 percent of events. ”Failure to open” accounts for 35 percent and “failure to remain closed (spurious opening)” for 23 percent of the reported events.

Degree of impairment: Six of the reported ICDE events were complete CCFs (all redundant components had failed in a short time interval and for the same cause). Partial CCF events i.e. at least two completely failed components in the observed population accounted for 33 percent. The remaining 60 percent of the events are not considered partial common cause failures, but they fall within the definition of an ICDE event.

Dominant **root causes** were "Design, manufacture or construction inadequacy" and "Internal to component piece part". This is consistent with the most important categories of **coupling factor** (i.e. factor behind dependency between the components) "Hardware" and "Maintenance." Regarding **detection methods**, the dominance of "testing / maintenance" (44 percent of the reported events) suggests that detection of ICDE events is quite successful. However, it can be further improved considering the high percentage of CCF events that were only revealed in demand situation (30 percent). The analysis concluded that good maintenance techniques could detect problems before component failure, even if the problems result from design deficiencies. The most frequently reported **corrective action** was "Specific maintenance / operational procedure" (all the codes in quotation marks represent ICDE coding).

Categorisation of **failure symptoms/manifestations** and **failure causes** was based on the verbal event descriptions and further engineering analysis for 92 ICDE events. The remaining twelve of the 104 events were omitted from this analysis because the degree of confidence about multiple failures resulting from the same cause and/or in a short time interval was low.

Three **failure symptoms/manifestation** types were identified as dominant in the data:

1. Movement of the breaker mechanism is impeded by *insufficient/inadequate lubrication*, more than half of them affecting the latching mechanism. This suggests that improvements in the maintenance practices should be concentrated upon checking the status of lubrication more regularly.
2. Movement of the breaker mechanism is impeded by *wear, broken, bent, or loose parts, friction, binding, resulting from excessive stress, or faulty installation*. Mechanical wear is the dominant failure mechanism in this failure symptom/ manifestation category. Wear mostly affected the latching mechanism, coils and relays. Besides deficient maintenance/test procedures and practices, insufficient awareness of aging of breaker piece parts also contributes significantly to this category.
3. *Various electrical problems*, like defective coils and command circuits, wiring faults, loose wires, poor contacts, blown fuses. Defective coils and defective command circuits are the dominant failure mechanisms in this category. The events are mostly caused by deficiencies in design, construction and manufacturing.

Deficiencies during operation contributed to 48 percent of the **failure causes**, mainly due to "*Deficient maintenance procedures/practices"* which accounted for 33 percent of the failure causes. In many cases, test and maintenance intervals were too long to detect the failure mechanism before multiple components were affected. The fact that about one third of the failures were detected on demand suggests that testing practices/techniques may not always have been capable of detecting failure mechanisms during their development. The other 52 percent of failure causes were design, construction, manufacturing deficiencies, mainly due to failure cause category "Deficiencies in design of hardware". Most of these failures were caused by *mechanical wear*.

Procedures and maintenance related corrective actions had been taken by the utilities in consequence of 63 percent of the ICDE events, although deficient procedures and maintenance activities were involved in only 33 percent of the events. This suggests that the operators consider that improved procedures and

maintenance practices can be an effective and efficient defense even against hardware related failures. One example is failures due to the specification of an unsuitable lubricant by the manufacturer; corrective action included the specification of a different lubricant as well as improved maintenance/test procedures and practices.

The high share of the procedure and maintenance related corrective actions underlines the paramount importance of continued reviews and improvements of existing maintenance and operating procedures and practices in order to enhance the plant-specific CCF defence.

ACRONYMS

AC	Alternating Current
BWR	Boiling Water Reactor
CB	Switching Devices and Circuit Breakers
CCF	Common Cause Failure
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee on the Safety of Nuclear Installations
DC	Direct Current (Continuous current)
FC	Failure to Close
FO	Failure to Open
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
HSE	Health and Safety Executive (UK)
HSK	Hauptabteilung für die Sicherheit der Kernanlagen (Switzerland)
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)
JNES	Japan Nuclear Energy Safety Organisation (Japan)
KAERI	Korea Atomic Energy Research Institute (Republic of Korea)
LOCA	Loss-of-Coolant Accident
LOSP	Loss of Offsite Power
MCC	Motor Control Centre
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (USA)
OECD	Organization for Economic Cooperation and Development
OP	Observed Population
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment

PWR	Pressurized Water Reactor
RPS	Reactor Protection System
RTB	Reactor Trip Breakers
SKI	Sweden Nuclear Inspectorate (Sweden)
SO	Spurious Open
STUK	Finish Centre for Radiation and Nuclear Safety (Finland)
UV	Under voltage

GLOSSARY

(Ref. 2 to 5)

Common Cause 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 failure. The component has completely failed and will not perform its function. For example, if the cause prevented a pump from starting, the pump has completely failed and impairment would be complete. If the description is vague this code is assigned in order to be conservative.

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

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

Coupling Factor/Mechanism*:* The coupling factor field describes the mechanism that ties multiple impairments together and identifies the influences that created the conditions for multiple components to be affected.

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

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

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

Failure Mechanism: The history describing the events and influences leading to a given failure.

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

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

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

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

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

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

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

Timing Factor: This is a measure of the "simultaneity" of multiple impairments. This can be viewed as an indication of the strength-of-coupling in synchronizing failure times.

1. INTRODUCTION

This report presents an overview of the exchange of common cause failure (CCF) data of switching devices and circuit breakers (CB) among several countries. The objectives of this report are:

- To describe the data profile in the ICDE database for CB and 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.

The ICDE Project was organized to exchange CCF data among countries. A brief description of the project, its objectives, and the participating countries, is given in Section 2. Section 3 presents the definition of common cause failure and the ICDE event definitions. Section 4 presents a description of the CB, and Section 5 summarizes the coding guidelines for this component. Sections 6 and 7 contain the results of the study. Section 8 contains the summary and conclusions of the study.

2. ICDE PROJECT

2.1 Background

Common-cause-failure (CCF) events can significantly impact the availability of safety systems of nuclear power plants. In recognition of this, CCF data are systematically being collected and analysed in several countries. A serious obstacle to the use of national qualitative and quantitative data collections by other countries is that the criteria and interpretations applied in the collection and analysis of events and data differ among the various countries. A further impediment is that descriptions of reported events and their root causes and coupling factors, which are important to the assessment of the events, are usually written in the native language of the countries where the events were observed.

To overcome these obstacles, the preparation for the international common-cause data exchange (ICDE) project was initiated in August of 1994. Since April 1998, the OECD/NEA has formally operated the project. The Phase II had an agreement period covered years 2000-2002, phase III covered the period 2002-2005 and phase IV 2005-2008. Member countries under the Phase IV Agreement of OECD/NEA and the organizations representing them in the project are: Canada (CNSC), Finland (STUK), France (IRSN), Germany (GRS), Japan (JNES), Korea (KAERI), Spain (CSN), Sweden (SKI), Switzerland (HSK), United Kingdom (HSE), and United States (NRC). Phase V is planned to begin in April 2008.

2.2 Objectives of the ICDE Project

The objective of the ICDE activity is to provide a framework for a multinational co-operation:

a) collect and analyse Common-Cause Failure (CCF) events over the long term so as to better understand such events, their causes, and their prevention;

b) 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;

c) 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;

d) generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries; and

e) use the ICDE data to estimate CCF parameters.

2.3 Scope and Status 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, batteries, control rod drive mechanisms (CRDA), circuit breakers, level measurement, heat exchangers, etc.

CSNI reports have been produced for centrifugal pumps, diesel generators; motor operated valves, safety & relief valves, check valves and batteries (See section 2.4). This report is about switchgear and breakers. Reports on level measurement equipment and control rod drive assemblies will be finalised in 2008. Work on heat exchangers has started and will continue during the fifth ICDE project period 2008-2011.

2.4 Reporting and Documentation

The ICDE project has produced the following reports, which can be accessed through the OECD/NEA CSNI web site for CSNI reports [1]:

- Collection and analysis of common-cause failure of centrifugal pumps [NEA/CSNI/R(99)2]. Issued September 1999.
- Collection and analysis of common-cause failure of emergency diesel generators [NEA/CSNI/R(2000)20]. Issued May 2000.
- Collection and analysis of common-cause failure of motor-operated valves [NEA/CSNI/R(2001)10]. Issued February 2001.
- Collection and analysis of common-cause failure of safety valves and relief valves [NEA/CSNI/R(2002)19]. Issued October 2002.
- Collection and analysis of common-cause failure of check valves [NEA/CSNI/R(2003)15]. Issued February 2003.
- Collection and analysis of common-cause failure of batteries [NEA/CSNI/R(2003)19]. Issued September 2003.
- ICDE General Coding Guidelines [NEA/CSNI/R(2004)4]. Issued January 2004.
- Proceedings of ICDE Workshop on the qualitative and quantitative use of ICDE Data [NEA/CSNI/R(2001)8]. Issued November 2002.

2.5 Database management

Data are collected in an MS.NET based database implemented and maintained at ES-Konsult, 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.

2.6 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 guideline and in the component specific guidelines. Component specific guidelines are developed for all analysed component types as the ICDE plans evolve [2].

2.7 Protection of Proprietary Rights

Procedures for protecting confidential information have been developed and are documented in the Terms and Conditions of the ICDE project [6]. The co-ordinators in the participating countries are responsible for maintaining proprietary rights according to the stipulations in the ICDE Terms and Conditions [6]. The data collected in the database are password protected and are only available to ICDE participants who have provided data.

3. DEFINITION OF COMMON-CAUSE EVENTS AND ICDE EVENTS

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

- 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, and 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 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, "Common Cause Failure Data Collection and Analysis System, Vol. 1, NUREG/CR-6268": [3]

- Common-Cause 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.

The data collection in the ICDE project comprises complete as well as potential CCF. To include all events of interest, an 'ICDE event' is defined as follows:

- ICDE Event: Impairment1 of two or more components (with respect to performing a specific function) that exists over a relevant time interval2 and is the direct result of a shared cause.

The ICDE data analysts may add interesting events that fall outside the ICDE event definition but are examples of recurrent - eventually non random - failures.

---

1 Possible attributes of impairment are the following:

- Complete failure of the component to perform its function
- Degraded ability of the component to perform its function
- Incipient failure of the component

Default is component is working according to specifications.

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

4. COMPONENT DESCRIPTION

4.1 General Description of the Component

According to the Coding Guidelines for Switching Devices and Circuit Breakers (CB) [4], the CBs of interest are those that belong to (Low/Medium Voltage) Electrical Distribution Systems (busbar/motor control centre (MCC)3 feeder and load breaker) and Reactor Trip Breakers.

The Medium voltage circuit breakers considered here are feeder circuit breakers to smaller electrical distribution centres, circuit breakers between two medium voltage buses, and the feeder circuit's breakers from off-site power. Circuit breakers that supply individual components are not included in this analysis, i.e.: Diesel Generator (DG), Motor Operated Valve (MOV), and Motor Pump (MP) breakers are included within their component boundaries.

Included within the Low voltage circuit breakers are the circuit breakers located at the motor control centres (MCC) and the associated power boards that supply power specifically to any low voltage equipment.

The reactor trip breakers (RTBs)4 are part of the reactor protection system (RPS), and supply power to the control rod drive mechanisms. Both AC and DC breakers are used for the RTBs. On a reactor trip signal, the breakers will open, removing power from the control rod drive mechanisms. The control rods will then unlatch and drop into the reactor core due to gravity.

The following systems are to be evaluated:

- Emergency Distribution System:
  - AC Low voltage (up to 1000V)
  - AC Medium voltage (1KV – 11KV)
  - DC Low voltage (up to 600V)
- AC Onsite Power Distribution System:
  - AC Low voltage (up to 1000V)
  - AC Medium voltage (1KV – 11KV)
  - DC Low voltage (up to 600V)
- Reactor Protection System (Reactor Trip Breakers, low voltage).

---

3 Motor Control Centre: a floor mounted assembly of one or more enclosed vertical sections having a common horizontal power bus and principally containing combination motor starter units. These units are mounted one above the other in vertical sections. The sections may incorporate vertical buses connected to the common power bus, thus extending the common power supply to the individual units. Units may also connect directly to the common power bus by suitable connections.

4 Reactor Trip Breakers correspond to some PWR plants (Westinghouse, Babcock&Wilcox, Combustion Engineering and similar design).

4.2 Component Boundaries

The boundary for the medium voltage circuit breaker is the breaker itself and the equipment contained in the breaker cubicle. AC circuit breakers have over current protection that is integral to the breaker unit. External equipment used to provide additional protection by monitoring parameters such as under voltage, differential faults, ground faults, and other protection schemes as required for circuit breakers are also considered part of the circuit breaker. In addition, remote circuitry used for circuit breaker operation is considered integral to the function of the circuit breaker for failure analysis. It includes all sensing devices, cabling, and components necessary to process the signals and provide control signals to the individual circuit breaker.

The MCCs and the power boards are not included in the boundary for low voltage circuit breaker except for the load shedding and load sequencing circuitry/devices, which are in some cases physically located within the MCC. Load shedding of the safety bus and subsequent load sequencing onto the bus of vital electrical loads is considered integrated to the Low Voltage circuit breaker function and is therefore considered within this study. All instrumentation, control logic, and the attendant process detectors for system initiations, trips, and operational control are included.

In general, the switching devices / circuit breakers include the contactors, actuator, latching mechanism, control and instrumentation installed on the switching device, enclosures, compartments (containing for example SF6, oil or vacuum), and the power terminations which are either electrical terminations or pneumatic lines.

The component boundary is illustrated in Figure 1.

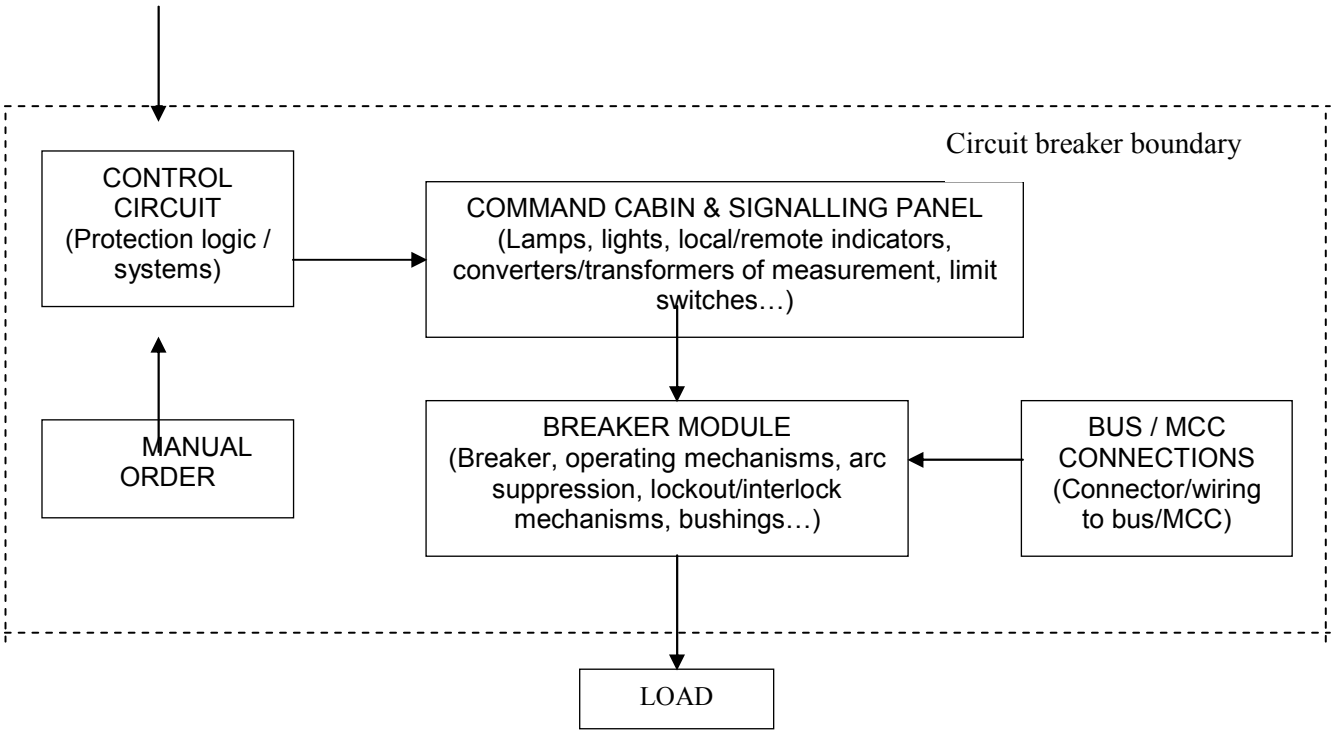


Figure 1. Physical boundary of breakers

The component, RTB, is defined as the breaker itself as well as the undervoltage and shunt trip devices. The circuitry that provides input power to the breakers is not viewed as part of the breaker.

Figure 2 shows the RTB arrangement for various vendors and designs [5].

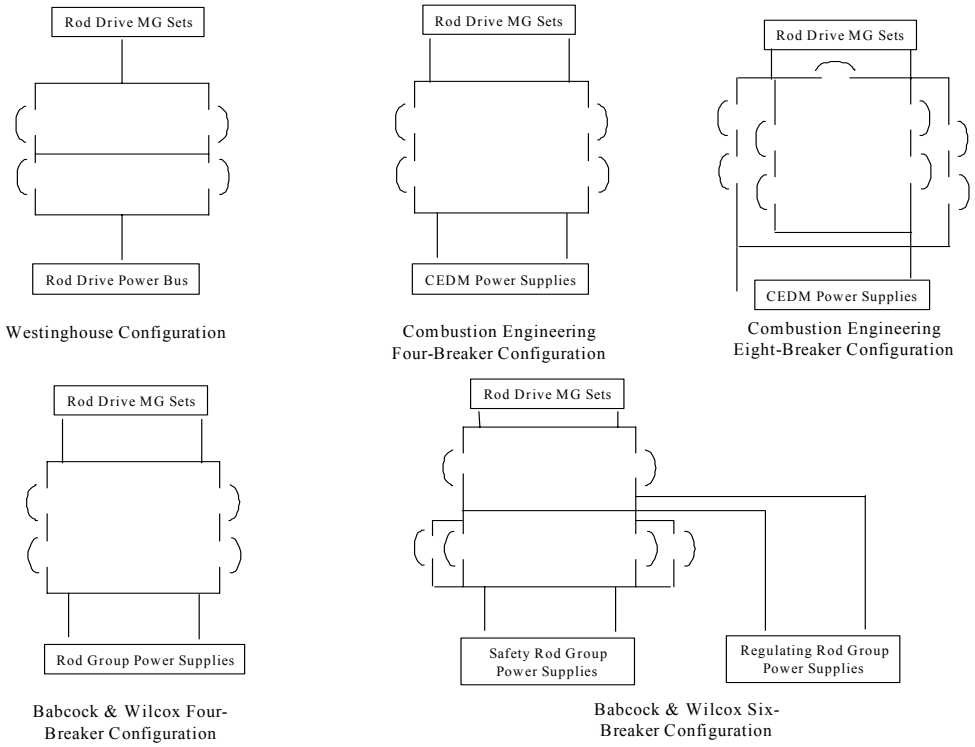


Figure 2. Reactor trip breakers

4.3 Event Boundary

The mission for the switching device / circuit breaker is to maintain, connect or break electrical current as demanded. Failure of switching device / circuit breaker occurs if it fails to maintain, connect or break electrical current.

5. BREAKER EVENT COLLECTION AND CODING GUIDELINES

5.1 Coding Rules and Exceptions

1. In general, the definition of the ICDE event is given in Section 2 of the General ICDE Coding Guidelines [2].

2. Some reports may discuss only one actual failure, and do not consider that the same cause will affect other Switching Devices / Circuit Breakers, but the licensee replaces the failed component on all switchgears / breakers as a precautionary measure. This event will be coded as incipient impairment of the components that did not actually fail.

3. Inoperability due to seismic or electrical separation violations will not be included, unless an actual failure has occurred.

5.2 Functional Failure Modes

The functional breaker failure modes are [5]:

1. Failure to Open (FO): Closed breakers that have a demand to open and fail to open. This includes manual operation, automatic operation such as load sequencing circuitry, RPS scram, and overcurrent/undervoltage conditions where the breaker fails to open.

2. Failure to Close (FC): The breaker did not close or would not have been able to close if a close signal had been generated. In the case of RTB, they are tested to determine the closing time. If the closing time is too slow, the breakers must be worked on and re-tested. How far off of allowable closing time is considered a failure: the usual guidance here is if parts are indicated to be broken/worn/failed, and/or the closing time is greater than 10% over, a failure is recorded.

3. Spurious Operation (SO): The breaker opened when it should have stayed closed or closed inadvertently, because of a breaker fault within the component boundary. Some reports state that the breaker was found in the tripped condition; these are considered spurious operation. Also included are spurious operations of the breaker due to personnel error, bumping the cabinet, or radio interference.

For the purposes of this CCF study, a personnel error resulting in more than one functionally inoperable RTB is considered a CCF failure, even if there is no component malfunction and the component is not demanded.

Some event reports indicate that breakers have spuriously actuated due to a system fault, which causes an overcurrent or undervoltage condition, and the breaker trips as designed for protective function. Any situation where the breaker acts as designed will not be coded as a failure. However, a fault within the circuit breaker component boundary that causes an inadvertent trip or closure would be a Spurious Operation.

6. OVERVIEW OF DATABASE CONTENT

CCF data have been collected for Switching Devices and Circuit Breakers (CB). Organisations from Canada, Finland, France, Germany, Spain, Sweden, United Kingdom, and United States have contributed to this data exchange. One-hundred-four (104) ICDE events were reported from nuclear power plants (pressurized water reactors, boiling water reactors, Magnox and advanced gas reactors). The data span a period from 1983 through 2004. The data are not necessarily complete for each country through this period.

Collecting these events has 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. Particularly this bottom-up work is rather resource intensive. However, depending on the detail of description in licensee event reports and plant maintenance sheets available information on CB events is very limited sometimes and consequently, deeper analysis and conclusions are limited in these cases.

The distributions of events in the following section are strictly based on the classes given in the ICDE coding guidelines [2]. In Section 7, a deeper engineering analysis of the events is presented.

6.1 Affected voltage levels

Table 1 shows the distribution of the collected events according to the classification referred to in Chapter 4.1, but without distinguishing between emergency distribution system and onsite power distribution system.

Table 1. Affected voltage levels

Low voltage AC	41	39%
Medium voltage AC	52	50%
Reactor Protection System	11	11%
Total	104	100%

Most of the collected events affected AC breakers of both medium and low voltage.

6.2 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 categorization of the general coding guidelines [2], with interpretation as presented in the Switching Device and Circuit Breaker coding guidelines (see Section 5.3) and summarized here.

- C denotes complete failure. The component has completely failed and will not perform its function. For example, if the cause prevents a breaker from opening, the breaker 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, time exceeded in opening/closing process over the normal observed, without endangering its function.
- 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 2 summarizes the reported ICDE events by failure mode and impact of failure. One-hundred and four ICDE events have been collected in the ICDE database. Six of them were complete CCF events when relating the number of completely failed components to the number of those exposed to the failure mechanism in question (an exposed population that is subset of the whole observed population). Only two of them were complete CCF events when relating the number of completely failed components to the number of components in the corresponding whole observed population. 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. In comparison to the number of the complete CCF events the number of partial CCF events is significantly higher.

Table 2. Failure mode distribution

FAILURE MODE	No. of ICDE events	Impact of failure [1)]	
		Complete CCF events	Partial CCF events
FO – Failure to open	36	1	7
FC – Failure to close	44	2	17
SO – Failure to remain closed (Spurious operation)	24	3	7
TOTAL	104	6	31

[1] Events with time factor or shared cause factor "low" are excluded. Of the 104 events collected in the database, twelve have time factor or shared cause factor "low".

The most common failure mode was "failure to close".

Complete CCF makes up a small fraction (6.7%) of the circuit breaker events.

The majority of the circuit breaker ICDE events classified showing at least one completely failed component are “failure to close” (33.7%), “failure to open” accounts for 18.3% and “spurious operation” for 17.3%. This category makes up 69.2% of the total.

For events without completely failed components, “failure to open” is the dominant failure mode (16.4%), followed by “failure to close” (8.7%) and “spurious operation” (5.8%). These categories make up 30.8% of the ICDE events.

6.3 Observed Population Size and Exposed Population

The breaker data collection is based on observed populations which often contain a large number of components. This is obvious as there is often a large number of sub-boards and associated breakers without a technical difference amongst them. However, for some of the identified events, the participating countries decided to define exposed populations as subsets of observed populations depending on the observed CCF mechanism/symptom. Table 3 summarizes the numbers of events related to a specific size of **exposed population** and related to the sizes of the respective **observed populations.** It can be seen, that in less then 30% of the observed events more than eight components were exposed to the observed CCF mechanism/symptom although the size of more than two thirds of the respective observed populations were larger than eight. Consequently, there are more events with low numbers of exposed components than with low sizes of observed populations**.** Obviously, there is a large share of CCF mechanisms/symptoms that affected less than the whole set of breakers put together in one observed population. This means, that even if there is no significant technical difference amongst a set of breakers – this was the reason why these breakers were put together in one observed population – a large share of CCF mechanisms/symptoms affected only a subset of them. This finding was not seen in former ICDE data collections on other types of components. The reason for this finding is not obvious.

Table 3. Exposed components in the observed population / observed population size distribution

EXPOSED COMPONENTS IN THE OBSERVED POPULATION			**OBSERVED POPULATION SIZE**		
No. of exposed components	**No. of events**	**% of total**	**Size of the observed population**	**No. of events**	**% of total**
Two	10	9.6%	Two	3	2.9%
Three	8	7.7%	Three	2	1.9%
Four	16	15.4%	Four	13	12.5%
Six	20	19.2%	Six	2	1.9%
Eight	20	19.2%	Eight	13	12.5%
More than eight	30	28.9%	More than eight	71	68.3%
TOTAL	**104**	**100%**	**TOTAL**	**104**	**100%**

6.4 Root Cause, Coupling Factor, Corrective Action and Detection Method

6.4.1 Root Cause

The general coding guidelines [2] 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 is suggested:

- C – State of other component(s) (if not modelled in PSA). The cause of the state of the component under consideration is due to state of another component. Examples are loss of power and loss of cooling.
- 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. 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 (sprays, floods, etc.) radiation, abnormally high or low temperature, vibration load, and severe natural events.
- H – Human actions. Represents causes related to errors of omission or commission on the part of plant staff or contractor staff. An example is a failure to follow the correct procedure. 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, piece part. Deals with malfunctioning of parts internal to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the environment of the component. Specific mechanisms include erosion/corrosion, 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 of procedures, such as change control.
- O – Other. The cause of events is known, but does not fit in one of the other categories.
- U – Unknown. This cause category is used when the cause of the component state cannot be identified.

Figure 3 summarizes the root causes of the analysed events as coded in the ICDE database.

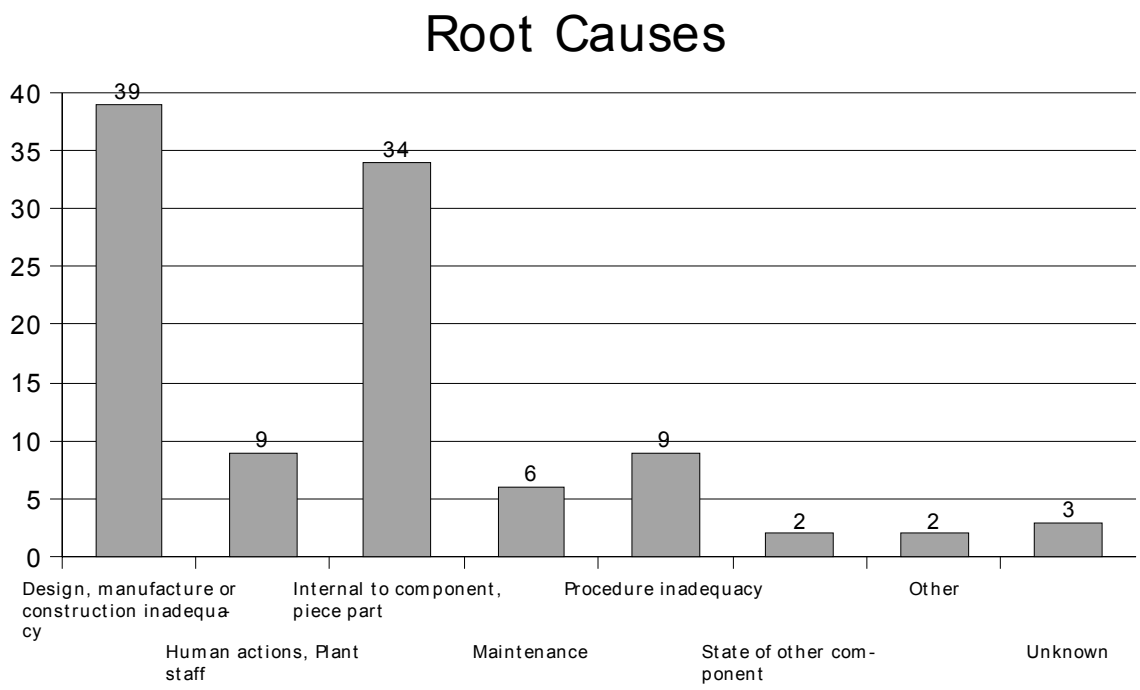


Figure 3. Root cause distribution

The dominant root causes based on the ICDE codes are, "Design, Manufacture or Construction inadequacy", accounting for 37% of the events and "Internal to component, piece part", accounting for 32% of the events.

6.4.2 Coupling Factor

The general coding guidelines [2] 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 of 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 – Maintenance/test (M/T) schedule. Components share maintenance and test schedules. For example, the component failed because maintenance 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 a calibration set point was incorrectly specified.
- OMF – M/T staff. Components are affected by a maintenance staff error.
- OP – Operation procedure. Components are affected by an inadequate operations procedure.
- OF – Operation staff. Components are affected by the same operations staff personnel error.
- 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.

Figure 4 shows the coupling factors of the analysed events as coded in the ICDE database.

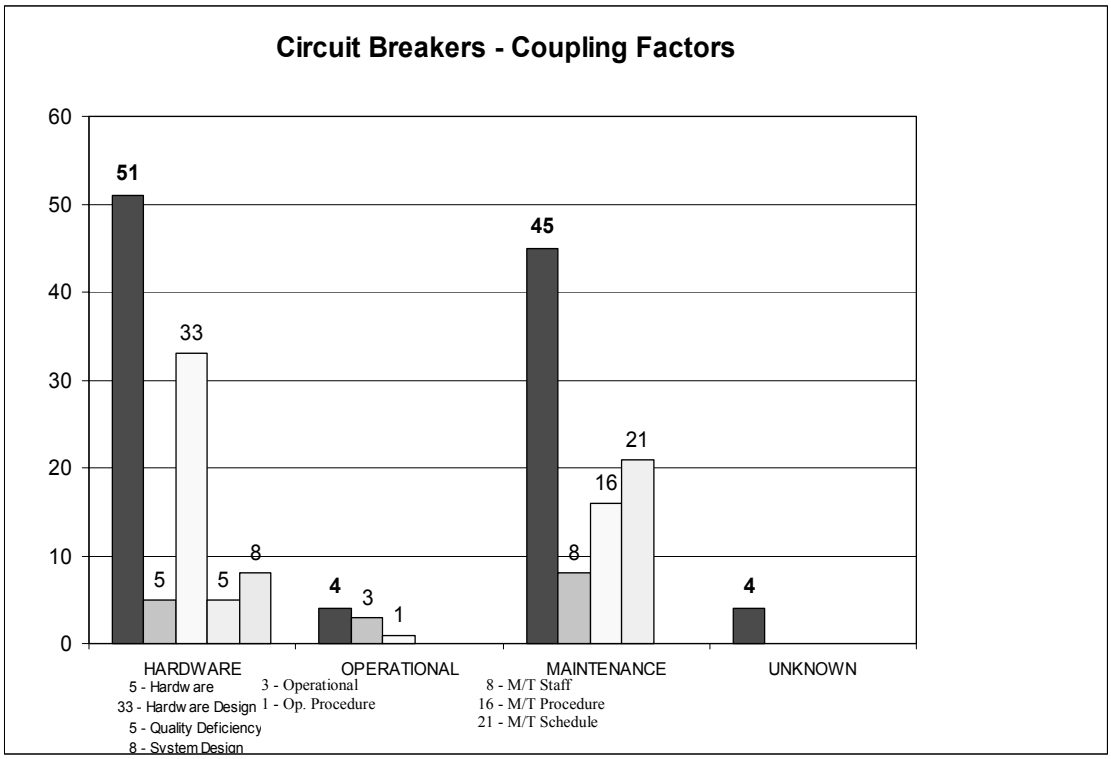


Figure 4. Coupling factor distribution

Some of the ICDE events have been classified using the top-level categories only, whereas for others also sub-categories have been used. To get a view of mechanisms involved with the different events, Figure 4 plots the top level coupling factor categories (brown bars), as well as the breakdown into the associated sub-categories and top-level category respectively. The green bars represent the sum of each class of categories.

The dominant coupling factor categories are "hardware", accounting for 49 % of the events, and "maintenance", accounting for 43 % of the events.

Within the “hardware” category, most events occurred due to “hardware design”, i.e. due to components sharing the same design and internal parts, rather than due to system design or manufacturing quality problems.

Within the “maintenance” category, most events occurred due to deficient maintenance/test procedures and practices

6.4.3 Corrective Actions

The ICDE general coding guidelines [2] define corrective action as follows. The corrective actions field describes the actions taken by the licensee to prevent the CCF event from re-occurring. The defence mechanism selection is based on an assessment of the root cause and/or coupling factor between the 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 items such as staggered testing and maintenance/operation staff diversity.
- G – Fixing of component.
- O – Other. The corrective action is not included in the classification scheme.
- U – Unknown. Adequate detail is not provided to make adequate corrective action identification.

Figure 5 summarizes the corrective actions of the analysed events as coded in the ICDE database.

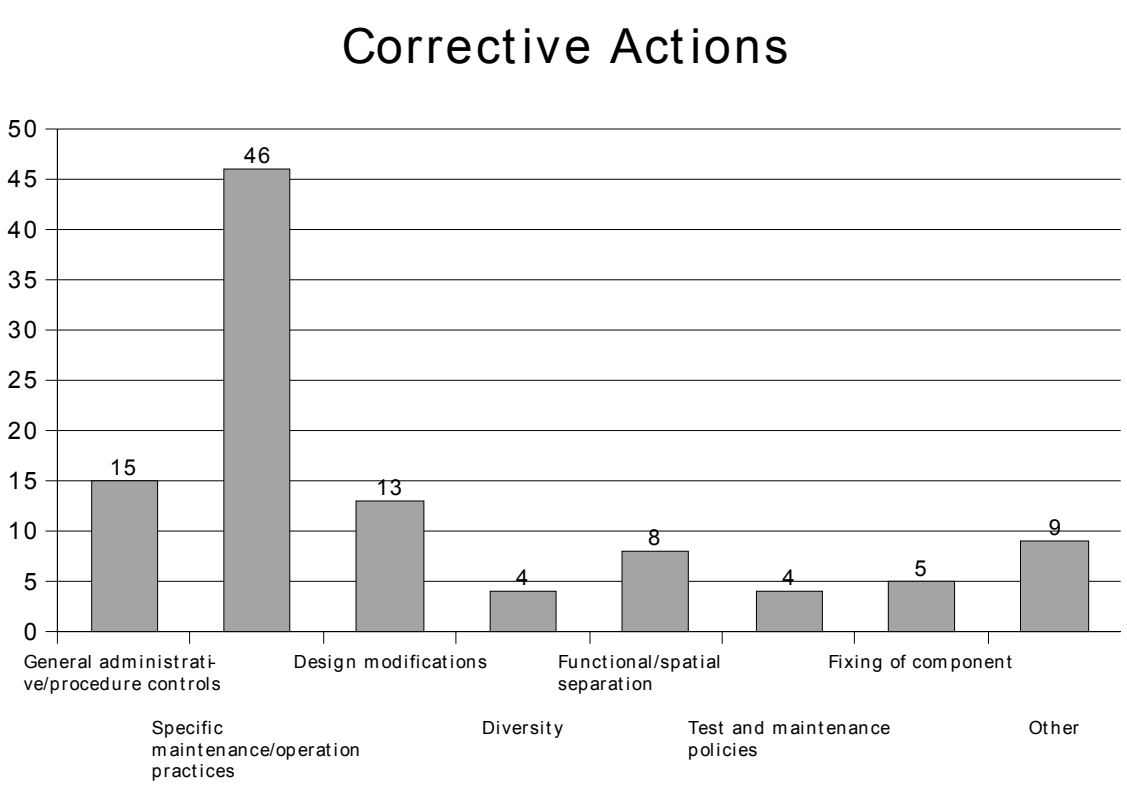


Figure 5. Corrective action distribution

The dominant corrective action, "Specific maintenance/operation practices", accounts for 44% followed by "General administrative/procedure control" and "Design modifications", accounting for 14% and 12% respectively.

General administrative/procedure control, specific maintenance/operation practices and test /maintenance policies together make up two-thirds of the taken corrective actions. About one third are aimed at improving hardware aspects.

6.4.4 Detection Methods

Figure 6 summarizes how the analysed events were detected.

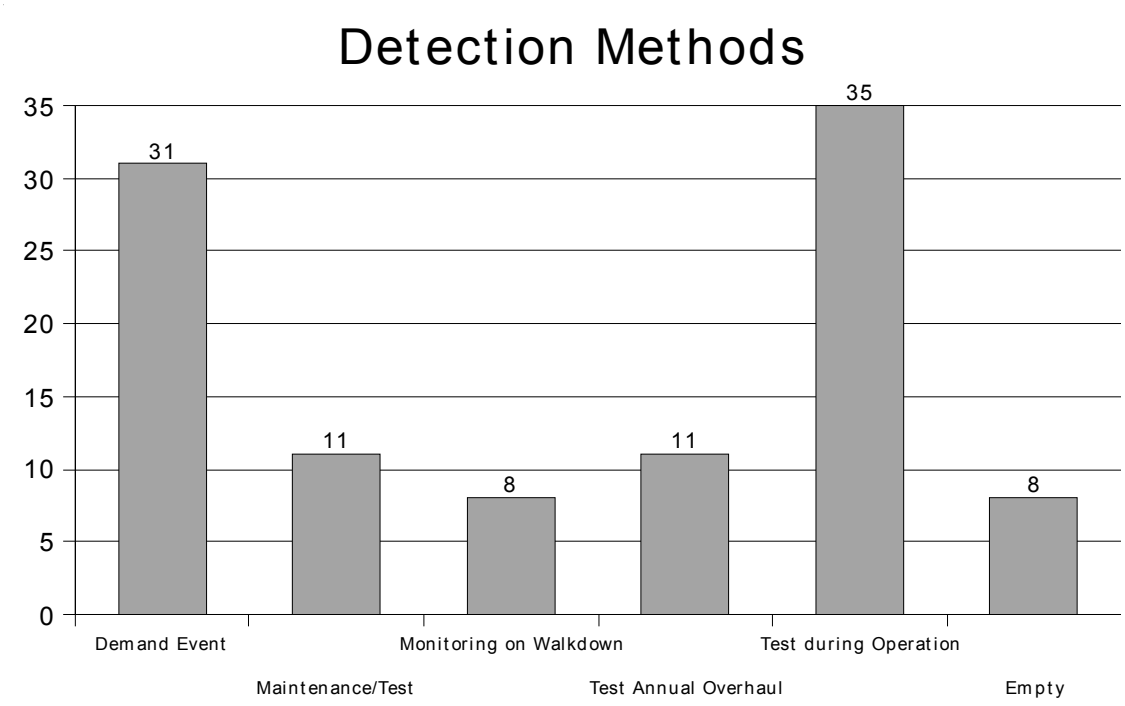


Figure 6. Detection method distribution

Fifty-seven ICDE events were discovered during test and maintenance activities (TA, TI, TL, TU, MA categories) and thirty-one in demand events, together representing 85% of the events collected. Test means that the equipment failure was discovered during the performance of a scheduled test. These tests are usually periodic surveillance tests. "Maintenance" means that the equipment failure was discovered during maintenance activities, usually during preventive activities.

That more than half of the events were discovered by testing and maintenance highlights the effectiveness of the employed procedures and practices for detecting common-cause failures. Eight events were detected through monitoring (MC, MW).

The failure mode of eight events was "spurious operation". No detection method was assigned to them. Three of these eight events were complete CFCs (relative to the number of exposed components).

No complete CCFs occurred in demand events, i.e. events where only the demand revealed the fault.

7. ENGINEERING ASPECTS OF THE COLLECTED EVENTS

The intention of this section is to provide the reader with a deeper qualitative insight in the database content beyond that obtained from using the database coding only (as performed in Section 6 of this report). Firstly, paragraph 7.1 presents an overview of the affected pieces or parts of circuit breakers based on the whole set of 104 events. In the subsequent paragraphs a detailed analysis of failure symptoms and causes is presented. For that purpose, all events classified with a low “time factor” or a low "shared cause factor" were omitted because the degree of confidence about multiple failures resulting from the same cause and/or in a short time interval is low in such cases. As a result of this screening process, 92 of the 104 reported ICDE events were reviewed in more detail with respect to the failure causes and the failure symptoms. In a second step, the review was confined to complete CCF events as defined in Section 6 of this report.

7.1 Pieces / Parts

Table 4 presents an overview of the affected pieces or parts of circuit breakers as they were identified in the analysed events. Many different piece parts were affected by the observed events, six of them with nine or more occurrences. The most frequently affected breaker part was the latching mechanism. The dominant cause was degraded or lacking lubrication, followed by incorrect installation. Relay failures were also fairly frequent, caused by aging or wear and by control logic problems.

Table 4. Affected pieces / parts

PIECES / PARTS	No of the events
Bearing	1
Circuit board / command circuit (diodes…)	1
Closing mechanism (in general)	9
Coil (undervoltage coil, shunt coil, trip coil)	11
Contacts	5
Digital trip unit	1
Enclosure (case, frame, casket)	2
Fuse	2
Latching mechanism	21
Limit switches	3
Lockout / interlock mechanism	1
Opening mechanism (in general) / trip device	10
Protection systems (instrumentation: sensors…)	9
Relays	12
Spring	3
Switch (cell, cutoff…)	3
Timer	1
Wires	4
Other (Breaker in general)	1
Other (Other component)	4
TOTAL	**104**

7.2 Assessment Basis

In the following sections, the 92 selected events, as described above, are analysed with respect to failure symptoms and failure causes. Appropriate failure symptom categories and failure cause categories are first identified by engineering binning of failure mechanisms derived from the verbal event descriptions. For the identification of failure causes, root causes are combined with coupling factors, because, by definition, it is the coupling factor that identifies the mechanism that ties multiple failures together 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 common cause failure categories.

Finally, the mapping of failure symptom categories onto failure cause categories is shown by the assessment matrix "Relationship of Failure Symptoms and Failure Cause Categories" (table 4). This matrix provides the basis for deriving insights and conclusions.

7.3 Failure Symptom Categories

Failure symptom categories are derived from the event descriptions. The following failure symptom categories were identified as being important to the analysis:

B1 Movement of the breaker mechanism is impeded by insufficient/inadequate lubrication.

B2 Movement of the breaker mechanism is impeded by broken, bent or loose parts, friction, binding, resulting from excessive stress, wear or faulty installation.

B3 Operation of the breaker is impeded by incorrect adjustment of setpoints/limit switches.

B4 Electrical problems caused e.g. by defective coils, defective command circuits, wiring faults, loose wires, poor contacts and blown fuses.

B7 Others (e.g. dirt, pollution, corrosion).

7.4 Failure Cause Categories

Two principal categories of failure causes are introduced:

Deficiencies in operation

This group comprises all ICDE events that involve human errors, expressed by a human error related root cause, or a human error related coupling factor. Note that, following this definition, events are included in this group if

- the root cause is human error related or
- the root cause is hardware related but human errors have created the conditions for multiple components to be affected by a shared cause, i.e. if the coupling factor is human error related.
- The root cause and coupling factor are human error related.

Three failure cause categories have been identified as being important in this group:

O1 Deficient procedures for maintenance and/or testing

O2 Insufficient attention to aging of piece parts

O3 Operator performance error during maintenance/test activities

Deficiencies in design, construction, manufacturing

This group comprises all events with hardware related root cause and hardware related coupling factor. Thus, an event is only included, for example, in category D (design deficiency) if the root cause is coded as "design", combined with any hardware related coupling factor, or if the coupling factor is coded as "hardware design" or "system design", combined with any hardware related root cause. Two failure cause categories have been defined for this group:

D Deficiency in design of hardware
C/M Deficiency in construction or manufacturing of hardware
D-MOD Deficient design modifications

7.5 Assessment matrix

The matrix "Relationship of failure symptoms and failure cause categories", Table 5, forms the basis for interpreting the collected data. The failure symptom categories as defined in Section 7.2 are assigned to the columns of the matrix, the failure cause categories as defined in Section 7.3 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 symptom/failure cause combinations. Note that these observations are based on the 92 events remaining after those with a "low" time factor and/or shared cause factor have been removed from the data set.

Table 5. Relationship of Failure Symptoms and Failure Cause Categories

	Failure Symptoms					
Failure Cause Categories	**B1** Movement of the breaker mechanism is impeded by insufficient /inadequate lubrication	**B2** Movement of the breaker mechanism is impeded by broken, bent or loose parts, friction, binding, resulting from excessive stress, wear or faulty installation	**B3** Operation of the breaker is impeded by incorrect adjustment of setpoints/limit switches	**B4** Electrical problems due to defective coils, defective command circuits, wiring faults, loose wires, poor contacts, blown fuses	**B5** Others (e.g. dirt, pollution, corrosion)	**Total**
Deficiencies in operation (root cause or coupling factor are human error related)	17	10	6	9	2	44
O1 Deficient maintenance/test procedures	16	5	4	4	1	30
O2 Insufficient attention to aging of piece parts	1	4		4		9
O3 Operator performance error during maintenance/test activities		1	2	1	1	5
Design, construction, manufacturing deficiencies (root cause and coupling factor are hardware related)	12	13	5	18		48
D Deficiencies in design of hardware	12	10	5	12		39
C/M Deficiencies in construction/ manufacturing of hardware		3		3		6
D-MOD Deficient design modifications				3		3
Total	29	23	11	27	2	92

The following observations are made from Table 5:

7.5.1 Failure cause categories

Deficiencies in operation are cause of 48% of the failures, mainly due to cause category O1, "Deficient maintenance procedures". Yet, there is also a significant contribution from category O2, "Insufficient attention to ageing of piece parts". Seven of the nine events in this category were demand events, two occurred in tests during operation. They all led to complete failure of at least one component of the exposed population, seven of them led to multiple complete failures. The last two observations justify the introduction of O2 as a separate category.

The other 52% of failure causes are design, construction and manufacturing deficiencies, mainly due to failure cause category D, "Deficiencies in design of hardware".

7.5.2 Failure symptom categories

B1. "Movement of the breaker mechanism is impeded by insufficient/inadequate lubrication" is the dominant failure symptom category, accounting for nearly one third of the failure symptom categories. More than half of the lubrication problems are caused by deficiencies in operation, in many cases by inadequately long intervals for replacing lubricants. However, the share of problems caused by design deficiencies is nearly as high; this is surprising, it results from specification of unsuitable lubricants by the manufacturer.

B2. "Movement of the breaker mechanism is impeded by broken, bent or loose parts, friction, binding, resulting from excessive stress, wear or faulty installation" accounts for one quarter of the failure symptom categories, with "mechanical wear" being the dominant contribution. More than half of the problems are caused by design and manufacturing/construction problems. The remaining ones are caused by deficient maintenance procedures and by insufficient attention to aging of piece parts.

B3. "Operation of the breaker is impeded by incorrect adjustment of setpoints or limit switches" accounts for twelve percent of the failure symptom categories. The highest contribution is from "Deficiency in design of hardware", followed by "Deficient procedures for maintenance and/or testing" and "Operator performance error during maintenance/test activities".

B4: This category comprises electrical problems due to defective coils, defective command circuits, wiring faults, loose wires, poor contacts and spurious signals. Together they make up twenty-nine percent of the failure symptom categories. Dominant contributions are from defective coils and defective command circuits. The events in this category are mostly caused by deficiencies in design, construction and manufacturing. For defective command circuits there is also a significant contribution from deficient design modifications.

B5: Others. This category comprises various symptoms, like dirt, corrosion, pollution.

7.5.3 Human error involvement

- Human action involvement is high: "Deficiencies in operation", accounts for 48% of the failure cause categories. For all human performance related events improvements or additions to procedures, mostly for testing and maintenance, have been taken by the licensees.
- Procedures and maintenance related corrective actions have been taken for 54% of the hardware related failure cause categories, suggesting that the licensees believed that recurrence of the reported events could efficiently be made more unlikely by improved procedures and practices, mostly for maintenance.

- Only 24% of the events have both been caused by hardware problems and been corrected by hardware related measures. Changing practices may be a working and low-cost alternative in many cases, even for purely hardware related failures, so this low share is not surprising.
- A general remark is in order here: There are events for which a clear-cut distinction between human a aspects and hardware failure aspects is difficult. This is illustrated by the following example: Specification of adequate maintenance procedures including maintenance intervals is part of the maintainability design of any technical component. If non-compliance by the maintenance organization with such specifications causes a failure there clearly is human error involvement. If failures occur despite the observance by the operator of maintenance specifications the cause of such failures would be viewed as hardware related design error, because, for example, the progression of mechanical wear or the suitability of a lubricant had been misjudged by the designer. Finally, there is the situation that a plant has been in operation for an extended period of time, like most of the plants included in the ICDE data collection, but the operator has failed to adapt maintenance procedures to operating experience that suggests more stringent standards. Events falling in the categories "Deficiencies in design, construction, maintenance" but with procedure related corrective actions could have resulted from such situations. Unfortunately, most event descriptions related to such situations do not explain why the plant operator believed that hardware problems could be corrected by procedure related corrective actions, and whether such actions were effective.

7.5.4 Technical fault aspects

In 32% of the failure events, movement of the breaker mechanism is impeded by insufficient/inadequate lubrication, more than half of them affecting the latching mechanism. This suggests that improvements in the maintenance practices should be concentrated upon checking the status of lubrication more regularly.

In another 25% of the failure events movement of the breaker mechanism is impeded by wear, broken, bent or loose parts, friction, binding, resulting from excessive stress, or faulty installation. Mechanical wear is the dominant failure mechanism in this failure symptom/manifestation category. Wear mostly affected the latching mechanism, coils and relays. Besides deficient maintenance/test procedures and practices, insufficient attention to aging of piece parts also contributes significantly to this failure symptom/manifestation.

Various electrical problems, like defective coils and command circuits, wiring faults, loose wires, poor contacts, blown fuses account for 29% and adjustment problems of set points and limit switches for 12% of the failure events.

7.6 Complete CCFs

Based on the exposed population, there are six complete CCFs. Three of them involve two components. Three, six and sixteen components are involved in one of the three remaining cases each. Regarding the phenomena involved, two were caused by mechanical binding, one by a defective command circuit, one by a short circuit caused by maintenance work, one by failure to correctly adjust contacts, and one by a blown fuse. Depending on the modelling approach used, the latter can be viewed as residual CCF or as dependent failure. Four complete CCFs were hardware related, two involved human error. Half of the complete CCF events were “Failure to remain closed (spurious operation)”.

With the (whole) observed population as basis, there are only two complete CCFs, one double and one sixteen-fold CCF, caused by defective command circuit and, respectively, by mechanical binding.

No further conclusions on frequencies of symptoms and causes for complete CCFs can be drawn due to the small number of events.

8. SUMMARY AND CONCLUSIONS

Organizations from Canada, Finland, France, Germany, Spain, Sweden, United Kingdom and the United States contributed with CCF data of circuit breakers to this data exchange. One-hundred and four (104) ICDE events were reported from Nuclear Power Plants in these countries.

Ninety-two (92) of the 104 reported ICDE events were reviewed in more detail in Sections 6 and 7 of this report with respect to impact of failure, failure causes, failure symptoms and failure mechanism. All events classified with time factor or shared-cause factor "low" were screened out from this analysis to concentrate the effort to the most likely dependent failures.

Thirty-one of the ninety-two ICDE events retained for detailed analysis involve two or more completely failed components (the ICDE failure grades are incipient, degraded and completely failed).

In six events all components of the exposed population failed. Among these were three events involving double redundancy, and one event each involving redundancies of multiplicity three, six and sixteen. The small size of the sample does not permit corroborated conclusions regarding the effectiveness of higher redundancy for prevention of common-cause failures.

The most frequently occurring failure mode of circuit breakers was "failure to close".

Three failure symptoms/manifestations were identified as dominant in the data:

- Movement of the breaker mechanism is impeded by insufficient/inadequate lubrication, more than half of them affecting the latching mechanism. This suggests that improvements in the maintenance practices should be concentrated upon checking the status of lubrication more regularly.
- Movement of the breaker mechanism is impeded by wear, broken, bent or loose parts, friction, binding, resulting from excessive stress, or faulty installation. Mechanical wear is the dominant failure mechanism in this failure symptom/ manifestation category. Wear mostly affected the latching mechanism, coils and relays. Besides deficient maintenance/test procedures and practices, insufficient attention to aging of piece parts also contributes significantly to this category.
- Various electrical problems, like defective coils and command circuits, wiring faults, loose wires, poor contacts, blown fuses. Defective coils and defective command circuits are the dominant failure mechanisms in this category. The events are mostly caused by deficiencies in design, construction and manufacturing.

Deficiencies in operation contributed to 48% of the failure causes, mainly due to failure cause category "Deficient maintenance procedures/practices", which was involved in 33% of the failure causes. In many cases, test and maintenance intervals were too long to detect the failure mechanism before multiple components were affected. The fact that about one third of the failures were detected only when the component was demanded to work suggests that testing practices/techniques may not always have been capable of detecting some of the failure mechanisms during their development.

The other 52% of failure causes were design, construction, manufacturing deficiencies, mainly due to failure cause category "Deficiencies in design of hardware". Most of these failures were caused by mechanical wear.

Procedures and maintenance related corrective actions have been taken by the utilities in consequence of 63% of the ICDE events, although deficient procedures and maintenance activities were involved in only 33% of the events. This suggests that the operators thought that improved procedures and maintenance rules would be an effective and efficient defense, even against hardware related failures. One example is failures due to the specification of an unsuitable lubricant by the manufacturer, which were corrected by the specification of a different lubricant, but also by improved maintenance/test procedures and practices.

The high share of the procedure and maintenance related corrective actions underlines the paramount importance of continued reviews and improvements of existing maintenance and operating procedures and practices in order to enhance the plant-specific CCF defense.

9. REFERENCES

[1] NEA CSNI website, reports: http://www.nea.fr/html/nsd/docs/indexcsni.html.

[2] 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.

[3] Marshall, F.M., D. Rasmuson, and A. Mosleh. *Common Cause Failure Data Collection and Analysis System, Volume 1 – Overview*, U.S. Nuclear Regulatory Commission, NUREG/CR-6268, INEEL/EXT-97-00696. June 1998.

[4] Begoña Pereira; María Rosa Morales; Ian Morris; Fritiof Schwartz; Rafael Cid; Dale Rasmuson; Anna Oxberry. ICDECG08. *Coding Guidelines for Switching Devices and Circuit Breakers.* Draft 1.3, March 2005.

[5] Wierman, T.E., D.M. Rasmuson, and N.B. Stockton. *Common-Cause Failure Event Insights. Volume 4 – Circuit Breakers*, U.S. Nuclear Regulatory Commission, NUREG/CR-6819, INEEL/EXT-99-00613. March 2003.

[6] NEA/SEN/SIN/ICDE(2006)1. OECD Joint Project: International Common Cause Failure Data Exchange(ICDE), Amended Terms And Conditions For The Project Operation 2005-2008. 24 January 2006.