Unclassified **NEA/CSNI/R(2008)8**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **01-Jul-2008**

English - Or. English

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Cancels & replaces the same document of 23 June 2008

ICDE Project Report: Collection and Analysis of Common-Cause Failures of Level Measurement Components

Gesellschaft fur Anlagen-und Reaktorsicherheit mbH (GRS)
Germany

March 2008

JT03248508

English - Or. English

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. Since 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 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.

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:

A. Kreuser (GRS)

J. C. Stiller (GRS)

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 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 146 CCF events related to level measurement components spanning a period from 1983 through 2003. The function of the component "Level Measurement" is to monitor the liquid level in safety relevant vessels, tanks and piping. The events studied here were collected in the ICDE database. Organisations from Canada, Finland, France, Germany, 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.

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 causes, and engineering aspects like failure symptoms. The limitation is that the data is not necessarily exhaustive for each country throughout the study period.

Degree of impairment: Four percent of the examined ICDE events were complete CCFs (all redundant components had completely failed within a short time interval as a direct result of a shared cause). CCF events with at least two completely failed components in the exposed population within a short time interval as a direct result of a shared cause accounted for (22%). In the remaining (78%) of events less than two components of the exposed population failed completely within a short time interval as a direct result of a shared cause, but fall within the less stringent definition of an ICDE event: "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."

Five **failure modes** were specified for level measurement components in the ICDE coding guidelines: "Failure to indicate level during operation – failure to 'High' signal", "Failure to indicate level during operation – failure to 'Low' signal", "Failure to indicate changing level and failure to trigger limit switch

on demand", "Unstable signal (spurious activation)" and "General Failure" (instrument out of specification or instrument inoperability without specifying a detailed failure mode). The most frequently encountered failure mode of level measurement components is "General Failure", representing (74%) of events. "Failure to indicate level during operation – failure to 'Low' signal" accounts for about (14%) and "Failure to indicate changing level and failure to trigger limit switch on demand" for about (7%) of the reported events.

Root causes could not be specified for (49%) of the reported events. For these events root cause is classified as "other" or "unknown". For the remaining events the identified root causes distribute among four major categories: "State of other components" (13%), "Design, manufacture or construction inadequacy" (12%), "Human actions, plant staff" (10%) and "Procedure inadequacy" (8%). However, the categories of **coupling factor** (i.e. factor behind dependency between the components) could be identified for all reported events. The most important category is "Maintenance/test schedule" representing (43%) of the events. All together the "Operational and maintenance" categories account for (64%) of the events and "Hardware" for (32%).

Regarding **detection methods**, the dominance of "testing" (61%) and "monitoring in control room or on walkdown" (34%) suggests that detection of ICDE events is relatively successful. Only one event occurred during a real demand. It should be noted, however, that there is a high proportion of events with relatively long latent time (time from occurrence of failure to detection of failure). For about (20%) of the events latent time was one year/cycle or more. For about (5%) of the reported events latent time was even longer than four years. The most frequently reported **corrective action** was "Specific maintenance/operational practices" accounting for (53%) of the events. Charts and tables are provided showing the number of events for each of these event parameters.

Based on the definitions in the observed populations, the verbal event descriptions and further engineering analysis of the 146 ICDE events a deeper analysis was carried out to identify typical failure mechanisms or failure symptoms/manifestations and affected sub-components of the level measurement components.

In the majority of the analysed events the observed failure mechanisms affected the transmitters (98 events). In 83 events transmitters were out of calibration. The observed measurement errors could be fixed by calibration of the transmitters. According to event descriptions, mostly small deviations occurred, which did not compromise safety functions. Only in two events components failed completely. Both of these are complete CCFs. In four cases including these two complete CCFs it was found that the wrong calibration was due to using wrong preset setpoint values. This was caused by applying outdated procedures for adjusting the transmitters, errors in calculating preset setpoint values or erroneously not accounting for technical modifications of the plant when calculating preset setpoint values.

Other failure mechanisms concerning transmitters were technical defects of the transmitter, problems of electrical signal transmission or power supply and incompatibility of a new model.

In 47 events the failure mechanisms were related to gauge lines. Examples of observed failure mechanisms are:

- insufficient fluid level in reference columns, mainly due to leakages,
- insufficient filling and venting of gauge lines,
- clogging of gauge lines,
- erroneously interchanged pairs of gauge lines and
- valves put in wrong positions after test or maintenance.

Only one event concerned sensors, which were mounted in a wrong position.

In summary, the CCF mechanisms present in most events reported (e.g., transmitter drifts) usually do not pose a serious threat to the operability of safety systems, since they are typically discovered during tests or as conflicting level indications before a safety function is compromised.

However, mechanisms which remain undetected over a long period of time may pose a more serious threat to the availability of safety functions. This usually results from the fact that in many cases level measurement cannot be tested or is not tested as a whole for all relevant levels of the various vessels. Instead, only some parts, usually the transmitters, are tested periodically in short time intervals and because of that, the impairment of redundant level measurement systems may remain undetected. Therefore, level measurement testing should be aimed at covering, as far as possible, all relevant levels including verification that limit switches are triggered at correct levels. It is essential to examine systematically which parts of safety relevant level measurement devices are tested, which are testable and which are not testable. If a test as a whole is impossible, it should be examined which potential errors are not covered by the tests that are carried out, e.g., incorrect valve positions or miscalculated set points. Accounting for these aspects, strategies should be developed to avoid failures that remain latent over many years.

ACRONYMS

BWR	Boiling Water Reactor
CCF	Common Cause Failure
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee on the Safety of Nuclear Installations
GRS	Gesellschaft für Anlagen-und Reaktorsicherheit (Germany)
HSK	Hauptabteilung für die Sicherheit der Kernanlagen (Switzerland)
ICDE	International Common Cause Failure Data Exchange
IRSN	Institut de Radioprotection et de Sûreté Nucléare (France)
KAERI	Korea Atomic Energy Research Institute (Korea)
LOCA	Loss-of-Coolant Accident
NEA	Nuclear Energy Agency
NII	Nuclear Installations Inspectorate (UK)
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (USA)
NUPEC	Nuclear Power Engineering Corporation (Japan)
OECD	Organisation for Economic Cooperation and Development
OP	Observed Population
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reactor
PHWR	Pressurised Heavy Water Reactor
RPS	Reactor Protection System
SKI	Sweden Nuclear Inspectorate (Sweden)
STUK	Finish Centre for Radiation and Nuclear Safety (Finland)

GLOSSARY

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 Common Cause Failure Event: A Common Cause Event, in which all exposed components failed completely within a short time interval as 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: 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 of two or more components (with respect to performing a specific function) that exists over a relevant time interval and is the direct result of a shared cause.

Incipient: 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 observed population contains a fixed number of

components. Sets of similar observed populations form the statistical basis for calculating common cause failure rates or probabilities.

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

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

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

ICDE PROJECT REPORT
COLLECTION AND ANALYSIS OF COMMON-CAUSE FAILURES OF LEVEL MEASUREMENT COMPONENTS

1. INTRODUCTION

This report presents an overview of the exchange of level measurement Common Cause Failure (CCF) data among several countries. The objectives of this report are:

- To describe the data profile in the ICDE database for level measurement and to develop qualitative insights in the nature of the reported events, expressed by root causes, coupling factors, and corrective actions.

- To develop the failure mechanisms and phenomena involved in the events, their relationship to the root causes, and possibilities for improvement.

The ICDE Project was organised to exchange CCF data among countries. A brief description of the project, its objectives, and the participating countries, is contained in Section Two. Section Three presents the definitions of common cause failures and ICDE events. Section Four presents a description of level measurement and a short description of the sub components that comprise it. Section Five summarises the coding guidelines for this component. Section Six gives an overview over the data by tabulating failure modes, root causes, coupling factors, corrective actions and detection methods. In Section Seven a quantitative assessment of the collected data with respect to failure symptoms and causes is presented. Section Eight 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. Phase II covered an agreement period of the 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 organisations representing them in the project are: Canada (CNSC), Finland (STUK), France (IRSN), Germany (GRS), Japan (NUPEC), Korea (KAERI), Spain (CSN), Sweden (SKI), Switzerland (HSK), United Kingdom (NII), United States of America (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.

e) Use the ICDE data to estimate CCF parameters.

2.3 Scope of the ICDE project

The ICDE Project aims to include all possible events of interest, comprising complete, partial, and incipient CCF 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, circuit breakers, level measurement, heat exchangers etc.

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 Data collection status

Data are collected in a Microsoft .NET based databank implemented and maintained at ES-Konsult, Sweden, the appointed ICDE Operating Agent. The databank 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 generic 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 [5]. The co-ordinators in the participating countries are responsible for maintaining proprietary rights according to the stipulations in the ICDE Terms and Conditions [5]. 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 (e.g., 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, e.g., "Common Cause Failure Data Collection and Analysis System, Vol. 1, NUREG/CR-6268" [3]. This definition was adopted by the ICDE project [2].

- 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.

Data collection in the ICDE project also includes potential CCFs. To include all events of interest, an "ICDE event" is defined as follows:

- 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.

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

The function of the component "Level Measurement" is to monitor the liquid level in safety relevant vessels, tanks and piping. The output signal of level measurement equipment triggers protection signals in the subsequent reactor protection logic system in case of too high or too low level. According to the Coding Guidelines for Level Measurement [4], in ICDE data collection only those level measurement components are considered, which are part of the reactor protection system or part of the engineered safety feature actuation system. Level measurement components which are only used for operational needs (e.g., level control) are not considered.

The vessels, tanks and piping (in following called "systems") at which level measurement equipment is installed and data are collected for are:

- Pressuriser (PWR, PHWR).
- Steam generators secondary side (PWR, PHWR).
- Accumulators (PWR).
- Reactor refuelling water storage tanks (PWR, PHWR).
- Reactor coolant lines (mid-loop operation) (PWR).
- Containment sump (PWR, BWR).
- Reactor pressure vessel (PWR, BWR).
- Suppression pool (BWR).
- Reactor scram tanks (BWR).
- Calandria (PHWR).
- Chemical and Volume Control System (PWR).

Pressure transmitters/sensors are the central instrument of the component level measurement. The following types of transmitters/sensors are distinguished:

- Pressure difference transmitter with electric output signal (Barton-cell) (PDTE).
- Pressure difference transmitter of membrane type with electric output signal (PDTM).
- Pressure difference sensor, Bourdon type (PDSB).
- Sensor with ultrasonic measuring cell (SUMC).
- Sensor with capacitance measuring cell (SCMC).
- Pressure difference sensor with piezoelectric transducer (PDSP).
- Sensor with resistance thermometer (SRT).
- Becker core cooling monitoring (BCCM).
- Unspecified transmitter/sensor (level measurement).

4.2 Component boundaries

The component boundary in this data analysis includes the following: pressure gauge lines, isolation valves, transmitter or sensor, indicating instruments, and electronic limit switches.

Four sub-components which together build the component “level measurement” are defined:

- Pressure gauge lines including isolation valves.
- Transmitters or sensors.
- Indicating instruments.
- Electronic limit switches.

As redundancy degrees of these sub-components may differ in one system, e.g., one pair of pressure gauge lines can be connected to several transmitters, a separate observed population record should be defined for each sub-component.

4.3 Event boundary

Successful operation of level measurement is defined as monitoring the actual level and triggering limit switches if the level reaches predefined thresholds. These thresholds may be low level or high level thresholds.

5. LEVEL MEASUREMENT EVENT COLLECTION AND CODING GUIDELINES

5.1 Basic unit for ICDE event collection

ICDE data collection for level measurement should be done on sub-component basis. Observed failures of level measurement are related to the sub-component(s) which caused the failures. The basic set for level measurement data collection is the observed population of the affected sub-component. It is the totality of all level measurement sub-component equipment for one of the above defined "systems" as far as this equipment is not completely physically diverse. For Example, diverse transmitters which are connected to the same "system" belong to different observed populations. Depending on the observed failure mechanism, the number of exposed components (field C04 in the CCF event record) equals the observed population size in the observed population record of the affected sub-component. For example, for failure mechanisms concerning the pressure gauge lines, the number of pressure gauge lines is the number of exposed components.

For the majority of events sufficiently detailed information on sub-components was not available. For these events, data collection and coding was performed on the basis of components.

5.2 Time frame for ICDE event exchange

The minimum period of exchange should cover five years for each plant.

5.3 Functional failure modes

The functional failure modes are:

1. **Failure to indicate level during operation – failure to "High" signal** (FR High)

   Example for complete failure: Signal rises to full scale deflection although actual level in vessel does not change.

   Example for degraded failure: Signal drifts from actual value by more than some deviation that does not compromise the safety function.

   Example for incipient failure: Signal drifts from actual value less than this deviation but more than accuracy of measuring instrument.

2. **Failure to indicate level during operation – failure to "Low" signal** (FR Low)

   Example for complete failure: Signal drops to zero although actual level in vessel does not change.

   Example for degraded failure: Signal drifts from actual value by more than some deviation that does not compromise the safety function.

   Example for incipient failure: Signal drifts from actual value less than this deviation but more than accuracy of measuring instrument.

3. **Failure to indicate changing level and failure to trigger limit switch on demand** (FS)

   Examples for complete failure:

   - Signal keeps its value when level in vessel changes.
   - Transmitter or limit switch is so severely out of calibration or drifted that specified limits would not be triggered.

   Example for degraded failure: Drift or setpoint of limit switch off the required value by more than some deviation that does not compromise the safety function.

   Example for incipient failure: Drift or setpoint of limit switch off the required value, not compromising the safety function, but more than adjustment accuracy of equipment.

4. **Unstable signal (spurious activation)** (IO)

   Several events were not coded in-line with the coding guide. The failure mode was coded as "General Failure (Failure mode unspecified)".

5.4 Coding rules and exceptions

1. In general, the definition of the ICDE event given in section 2 of the General ICDE Coding Guidelines [2] applies.
2. All actual failures will be included (in either ICDE or independent event coding), if they could have occurred during a relevant operating mode or state.
3. Some event reports discuss only one actual failure, and do not consider that the same cause will affect other level measurements, but the licensee replaces the failed equipment on all level measurements as a precautionary measure. This type of event will be coded as a CCF, with a low (0.1) component degradation value for the components that did not actually fail. This also applies if it was decided to implement said replacement at a later time.
4. Administrative in-operability that does not cause the level measurement to fail to function is not included as a failure. An example is a surveillance test not performed within the required time frame.
5. In-operability due to human error or erroneous calibration/set up will be included (in either ICDE or independent event coding).
6. In-operability due to seismic criteria violations will not be included.

5.5 Experience with ICDE data collection on level measurement

In a workshop in connection with the 21st meeting of the ICDE Steering Group in Helsinki on June 21-23, 2005 the data that had been collected up to then were analysed. The workshop consisted of two parts. In the first part Observed Population Records from some example plants from all participating countries were analysed in three working groups. In the second part, the same working groups analysed some example CCF Event Records.

After each part of the workshop all participants came together and discussed the results of the evaluation. Some improvements for individual data records and general recommendations for description and coding of ICDE data were proposed. Based on the workshop's results proposals were made for future improvements of ICDE data collection. Recommendations on Observed Population data and on CCF event descriptions were developed and - after approval from the ICDE Steering Group - introduced in the coding guide for level measurement. Subsequently, some data records were improved by taking into account the recommendations listed in Appendix A.

6. OVERVIEW OF DATABASE CONTENT

CCF data have been collected for level measurement components. Organisations from Canada, Finland, France, Germany, Sweden, United Kingdom and United States have contributed to this data exchange. In the database 146 ICDE events from nuclear power plants (pressurised water reactors, pressurised heavy water reactors and boiling water reactors) were reported. The data span a period from 1983 through 2003. The data are not necessarily complete for each country through this period.

Available information on level measurement events sometimes is very limited. This means coding of events is difficult and sometimes ambiguous. Therefore, the numbers should be interpreted with great care.

In 42 events at least one component failed completely. In 34 events more than one component failed completely. For 32 of the 34 events the failures resulted from the same cause (coded as Shared Cause Factor "High"; see definition in [2]) and occurred simultaneously (coded as Time Factor "High"; see definitions in [2]). Six of these are complete CCFs, i.e., all components of the exposed population failed completely and had a code "High" for the Shared Cause and the Time Factor. Five complete CCF events occurred in exposed populations of size two and one in an exposed population of size four.

6.1 Failure mode

Table 6.1 summarises the ICDE events, used in this study, by failure mode. The definitions of the functional failure modes, as they apply to this data collection, are given in section 5.3. For about three-quarters of the events no detailed failure mode according to the coding guide has been given but the failure mode was classified either as "Instrument out of specification" or "Instrument inoperability". These events are counted as "General failure".

Table 6.1 **Failure mode distribution**

Failure Mode	**No. of events**	**Percentage of total**
Failure to indicate level during operation – failure to "High" signal (FR High)	3	2.1%
Failure to indicate level during operation – failure to "Low" signal (FR Low)	20	13.7%
Failure to indicate changing level and failure to trigger limit switch on demand (FS)	10	6.8%
Unstable signal (spurious activation) (IO)	5	3.4%
General failure (instrument out of specification or instrument inoperability)	108	74.0%
TOTAL	**146**	**100%**

Since "General failure" is the failure mode of the majority of events, no further analysis of coded failure modes is reasonable.

6.2 Impairment vector

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 [2], with interpretation as presented in the level measurement coding guidelines (see section 5.3) and summarised here.

- C denotes complete failure. The component has completely failed and will not perform its function.
- D denotes degraded. The component is capable of performing the major portion of the safety function, but parts of it are degraded.
- 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 did not 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.

As noted before, events with transmitters out of calibration were not coded in an entirely consistent way, i.e., for similar cases they were coded either as incipient or degraded impairments. Since events with transmitters out of calibration constitute the majority of events, no differentiation is made in this section between degraded and incipient failures.

Table 6.2 and Figure 6.1 summarise the numbers of ICDE events of different degrees of impairment.

Table 6.2 **Component impairment distribution**

Component Impairment Vector	**No. of events**	**Percentage of total**
Multiple complete failures with at least two completely failed components and both the Shared Cause Factor and the Time Factor coded as "High"	**32**	**21.9%**
• All components in the exposed population are complete failures (complete CCF)	6	4.1%
• All components in the exposed population are affected (at least incipient failures)	7	4.8%
At least one complete failure but not a multiple complete failure as defined above	**10**	**6.8%**
• All components in the exposed population are affected (at least incipient failures)	3	2.1%
No complete failures, only incipient or degraded components	**104**	**71.2%**
• All components in the exposed population are incipient failures	24	16.4%

Hence, in (23.3%) of the events all components of the exposed population were affected.

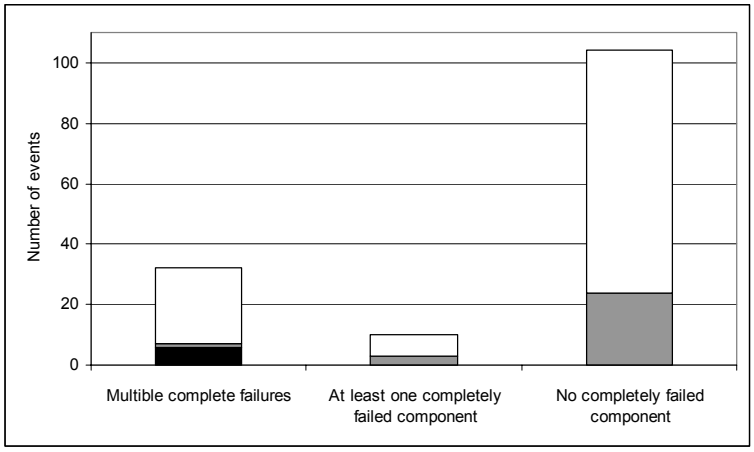

Figure 6.1 **Component impairment distribution**

The three categories are defined in Table 6.2. The number of complete CCFs is illustrated by a black bar. The numbers of events where all exposed components were affected (at least incipient failure) is illustrated by a grey bar. The number of other events is denoted as a white bar.

6.3 Size of observed and exposed populations

All events reported occurred in Observed Populations with three different (sub-) component types: "Level Measurement General" (12 events), "Pressure difference transmitter with electric output signal (Barton-cell)" (110 events) and "Pressure difference transmitter of membrane type with electric output signal" (19 events). In Table 6.3 the observed population size of the observed populations where CCF events took place is shown. Observed population size distributions are shown for all components, as well as for the components of the afore mentioned types.

Table 6.3 **Observed population size distribution**

	All		**Level Measurement General**		**Pressure difference transmitter with electric output signal (Barton-cell)**		**Pressure difference transmitter of membrane type with electric output signal**	
Observed population size	No. of events	Percentage	No. of events	Percentage	No. of events	Percentage	No. of events	Percentage
2	6	4.1%	4	33.3%	1	0.9%	1	5.3%
3	14	9.6%	-	0.0%	-	0.0%	13	68.4%
4	8	5.5%	2	16.7%	3	2.7%	1	5.3%
6	8	5.5%	3	25.0%	-	0.0%	3	15.8%
8	3	2.1%	-	0.0%	2	1.8%	1	5.3%
12	44	30.1%	1	8.3%	43	39.1%	-	0.0%
15	60	41.1%	-	0.0%	60	54.5%	-	0.0%
20	1	0.7%	-	0.0%	1	0.9%	-	0.0%
36	2	1.4%	2	16.7%	-	0.0%	-	0.0%
Total	**146**		**12**		**110**		**19**	
Average	**11.5**		**9.8**		**13.3**		**3.7**	

The exposed population is identical to the observed population in most events; only in 22 events involving Barton cells the exposed population is 4 in contrast to an observed population size of 12.

6.4 Root cause

The general coding guidelines [2] define root cause as 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 a common cause, the most readily identifiable cause. The following codes are used:

- C – state of other component(s) (if not modelled in PSA). The cause of the state of the component under consideration is due to the 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. 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 (sprays, floods, etc.) 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. 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. This 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. This 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 6.2 summarises the root causes of the analysed events as coded in the ICDE database. The numbers are also shown in Table B.1 in Appendix B.

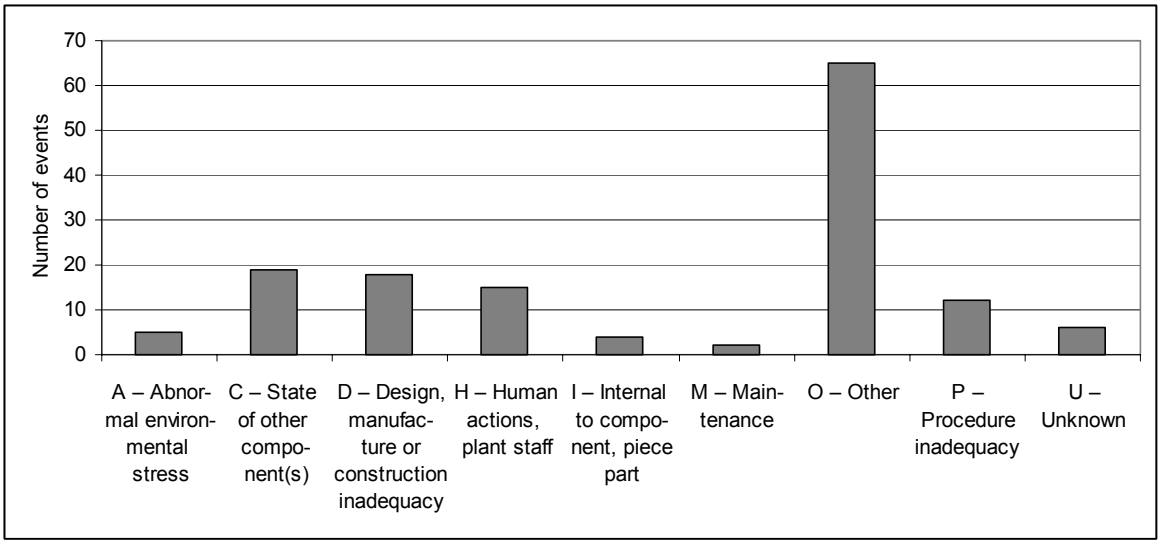

Figure 6.2 **Root cause distribution**

"Other" accounts for the largest number of the events (44.5%) "State of other component(s)", "Design, manufacture or construction inadequacy", "Human actions, plant staff" also give significant contributions.

The large number of events where the root cause was coded as "Other" indicates that the used categorisation is not very well suited for the level measurement events. It is remarkable that for 64 of the 65 events with root cause "Other" the failure mode is "General failure" without specification of one of the detailed failure mode categories. In these cases, nearly all event reports state that the level transmitters were found out of specification or out of calibration or drifted. This observation could be an indication that available information about malfunction of level measurement equipment often is not detailed enough to allow for a detailed categorisation of root causes.

6.5 Coupling factor

The general coding guidelines [2] define coupling factor as 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 setpoint 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.

Table 6.4 and Figure 6.3 show the coupling factors of the analysed events as coded in the ICDE database.

Table 6.4 **Coupling factor distribution**

COUPLING FACTOR	No. of events	Percentage
H – Hardware	15	10.3%
HC – Hardware design	9	6.2%
HQ – Hardware quality deficiency	1	0.7%
HS – System design	22	15.1%
O – Operational	9	6.2%
OP – Operation procedure	-	0%
OF – Operation staff	-	0%
OMS – Maintenance/test schedule	63	43.2%
OMP – Maintenance/test procedure	11	7.5%
OMF – Maintenance/test staff	10	6.8%
EI – Environmental internal	4	2.7%
EE – Environmental external	2	1.4%
U – Unknown	-	0%
TOTAL	146	**100%**

Table 6.4 shows that some of the ICDE events were classified using the top-level categories, while for most events sub-categories were used. Therefore, in Figure 6.3 the distribution of coupling factors is shown in terms of the top-level categories only, including the events associated to each sub-category within them. Some of the ICDE events have been classified as "H – Hardware" (in general), and others used "HC", "HS" codes. The same applies to "O – Operational" and "OP", "OF", "OMS", "OMP", "OMF" codes.

The distribution of the codes belonging to the three top categories is depicted in Figure 6.3.

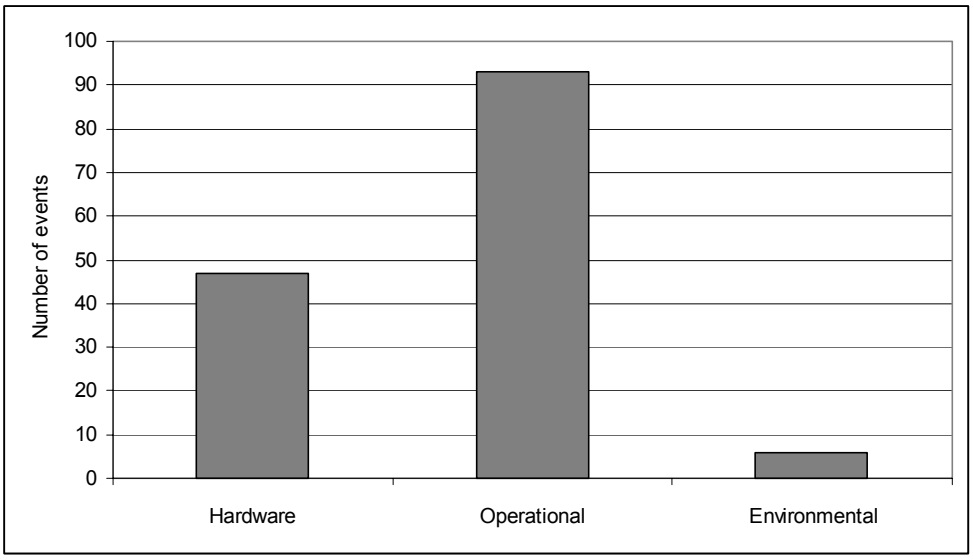

Figure 6.3 **Coupling factor distribution**

The coupling factor of (64%) of the events is operations related, (32%) is hardware related, while only (4%) is environmental.

About (68%) of the hardware related events were assigned to a sub-category. Amongst those, "System design" was dominant with (67%), while "Hardware design" contributed (28%).

About (90%) of the operations related events were assigned to a sub-category. Amongst those "Maintenance/test schedule" was dominant with (75%), while "Maintenance/test procedure" and "Maintenance/test staff" contributed each about (12%).

6.6 Corrective actions

The general coding guidelines [2] define corrective action as 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 6.4 summarises the corrective actions of the analysed events as coded in the ICDE database. The numbers are also shown in Table B.2 in Appendix B.

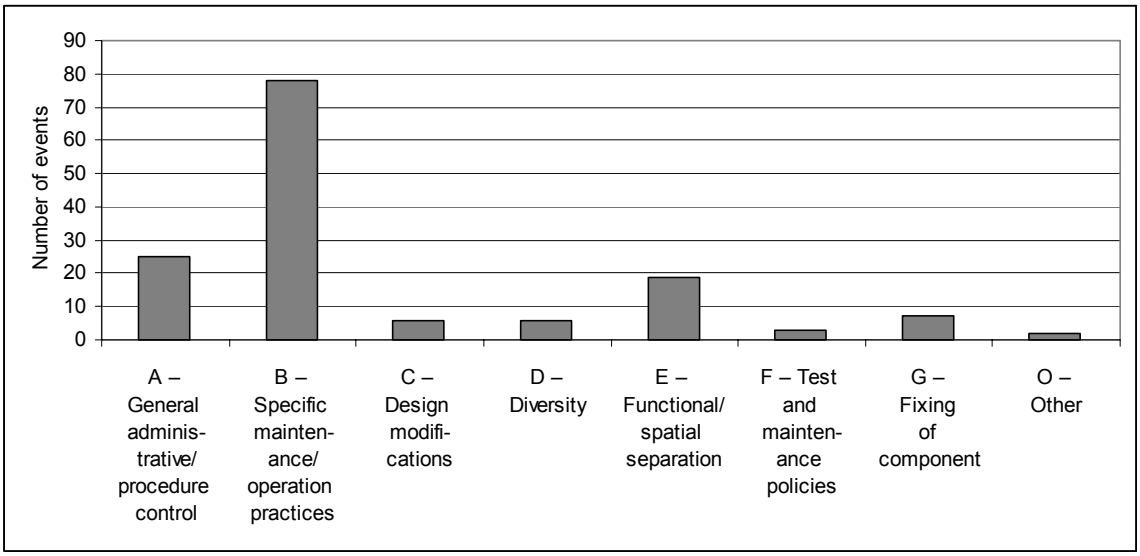

Figure 6.4 **Corrective action distribution**

The dominant corrective action, "Specific maintenance/operation practices", accounts for (53.4%). "General administrative/procedure control" and "Design modifications" account for (17.1%) and (13.0%), respectively.

6.7 Detection methods

Two different ways were chosen to code the detection method. While for most cases the code for each component was chosen identically as the code for the method by which the event had been first detected, for two events a different strategy was chosen: the detection method by which the event had first been detected was coded for the component which showed a complete failure only, while "MA - Maintenance/Test" was coded for the remaining components.

In the following only the detection method by which the event was first detected is considered. Figure 6.5 summarises the detection methods of the analysed events. The numbers are also shown in Table B.3 in Appendix B.

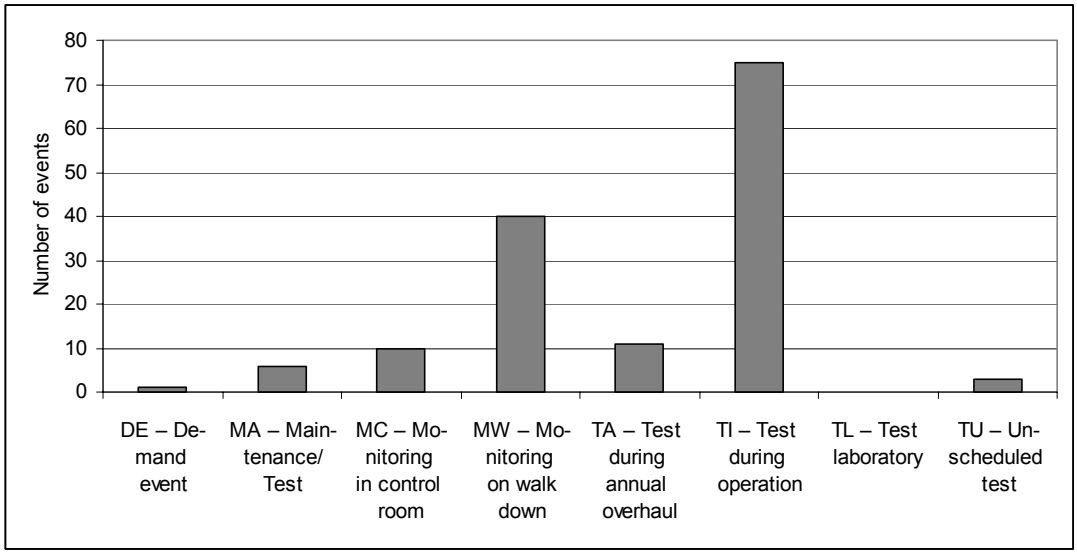

Figure 6.5 **Detection method distribution**

Most of the events were discovered during tests. Of these, the majority (about 51%) were discovered during operation, while (about 10%) were discovered in the course of tests during the annual overhaul or by unscheduled tests.

A significant share of events was detected by monitoring, mainly on walkdown but also in the control room. Most of these events were discovered by noting inconsistencies between levels indicated by different devices. A small fraction of events was discovered during maintenance activities. Only one event occurred during a demand.

It should be noted, however, that there is a high share of events with relatively long latent time (time from occurrence of failure to detection of failure). For (about 20%) of the events latent time was one year/cycle or more. For (about 5%) of the reported events latent time was even longer than four years. To understand the safety impact of these events an additional analysis was carried out. The results of this analysis are presented in Section 7.4 of this report.

7. ENGINEERING ASPECTS OF THE ICDE EVENTS

In this chapter typical failure mechanisms that were present in the events reported are discussed. The presentation of the failure mechanisms is structured according to their failure symptoms, e.g., transmitter out of calibration or gauge line clogging.

When analysing the events it became obvious that from different countries very different categories of events were reported, e.g., symptoms that occurred in the large majority of events of one country were not reported by other countries at all. This seems to be at least partly due to different reporting criteria.

Therefore, no statistical analysis of frequencies of specific symptoms, causes and consequences was performed and no analysis of the frequency of human factor related causes is presented.

Finally, the results of an additional analysis of events with very long latent times are presented.

7.1 Symptoms concerning transmitters

In most events (98) the symptom was a transmitter problem. Symptoms included:

- transmitter out of calibration,
- technical defects of the transmitter,
- problems of electrical signal transmission or power supply.

In the following these symptoms are discussed in further detail.

7.1.1 Transmitter out of calibration

Events showing transmitters out of calibration, i.e., when an observed measurement error could be fixed by calibration of the transmitters, constitute the majority (83) of cases. According to event descriptions, mostly small deviations occurred, which did not compromise safety functions, but also larger deviations were observed. Only in two events components failed completely. Both of these are complete CCFs, i.e., all exposed components failed and both Shared Cause Factor and Time Factor were coded as “High”.

The failures were typically discovered during tests of the transmitters or observed as conflicting level indications. In most of the descriptions of these events no cause for the wrong calibration of the transmitters was given; in some event descriptions it is explicitly stated that no investigations had been carried out to find the root cause. In some cases normal wear was assumed to be the root cause.

In four cases it was found that the wrong calibration was due to using wrong setpoint values. This was caused by applying outdated procedures for adjusting the transmitters, errors in calculating setpoint values or erroneously not accounting for technical modifications of the plant when calculating setpoint values. The two complete CCFs mentioned above fall into that category. In one of these cases a very large deviation occurred. This error had been present for four years. After its discovery test procedures were modified such that a similar event could be detected. In another case the deviation was small but still prohibited the triggering of a safety actuation feature.

In one case the wrong calibration was attributed to a drift that occurred when the system was warming up.

In a few cases it was stated that operational experience showed that specific models of transmitters show an increased tendency to drift out of calibration. The corrective measure taken was the replacement with a different model of transmitter.

7.1.2 Technical defects of the transmitter

In ten cases technical defects of the transmitter were found as reasons for an observed measurement error. Symptoms included defects of sensors or of power supply, loss of fill oil and corrosion. Corrective measures were replacement or repair of the transmitter. Only in one event more than one component failed completely within a short time interval as a direct result of a shared cause (Shared Cause Factor and Time Factor coded as "High").

7.1.3 Incompatibility of new type model

In one event a spurious activation of signals occurred because transmitters had been replaced by a new model with signal damping properties not fully compatible with the old models.

7.1.4 Electrical signal transmission or power supply

In four events the symptom was poor electrical contacts. These events occurred in three different plants from the same manufacturer in the same country. In two cases oxidation was the cause, while for the two remaining events no definite cause was reported. During one investigation into the event's cause it was discovered that transmitters belonging to different trains were connected to the same zero voltage feed. In all events at least one component failed completely.

7.2 Symptoms concerning sensors

In one event both of two redundant sensors were installed at wrong positions in the containment sump, such that they would have triggered at a level 0.4 m lower than designed. According to the event description it can be assumed that this error existed since plant construction.

7.3 Symptoms concerning gauge lines and reference columns

In the remaining events the symptom was a problem with gauge lines or reference columns including valves. Symptoms included:

- wrong fluid level in reference columns,
- insufficient filling and venting of gauge lines,
- clogging of gauge lines,
- valves in wrong position.

In the following these symptoms are discussed in further detail.

7.3.1 Wrong fluid level in reference columns

In thirteen events a wrong level in reference columns was the symptom. In most cases the level was too low. If causes were given in the event description, mostly leakages were named, but events were also attributed to insufficient filling after maintenance or testing.

In one event reference columns filled up to a solid water condition (level too high) due to a design error. This led to an inadmissibly large and non-conservative measurement error of steam generator level. As corrective action a design modification was planned.

In other cases no actual malfunctions were observed. However, during engineering planning work it was revealed that the condensation chambers of the reference columns were not mounted according to specifications. This error occurred during plant construction. During normal operation and in case of most LOCAs the error in the measured signal is small. Only in the long time phase of a LOCA inside the containment the deviation between the true and the indicated level can become very large. Administrative precautions for this case were implemented as corrective action.

7.3.2 Insufficient filling and venting of gauge lines

In six cases it was found that gauge lines were not properly filled and vented. They were discovered by implausible or conflicting level indications. Errors during maintenance or testing were named as causes. In five of these events at least two components failed completely within a short time interval as a direct result of a shared cause (Shared Cause Factor and Time Factor coded as "High").

7.3.3 Clogging of gauge lines

In four cases the clogging of gauge lines by corrosion products or dirt was the symptom. They were discovered by abnormal indications (frozen signals or large signal drifts). In one case increased reaction times of the signal to changing fluid levels were observed. All these events were events with at least two completely failed components (and Shared Cause Factor and Time Factor coded as "High"). As corrective action the sediments were removed.

7.3.4 Transmitter mounted at wrong positions

In three cases transmitters were mounted at a wrong position. As corrective actions the re-installation of the transmitters at the correct positions and the enlargement of the admissible measurement error were named.

7.3.5 Gauge lines erroneously interchanged

In three cases pairs of gauge lines were erroneously interchanged leading to an always high signal. The resulting failures of level measurement of accumulators existed since plant construction. The failure could not be detected in monthly periodic tests, because during these tests the level in the accumulator stays above the upper gauge line, so both gauge lines are always covered with coolant. Only during six-yearly tests when the accumulator is emptied can the error be detected. For all accumulators, where the error was present, the level measurement that triggers the closure of the isolation valve to avoid injection of nitrogen gas into the primary circuit was completely inoperable.

7.3.6 Instrumentation nozzle design fault

Due to a design error of the bottom instrumentation nozzle of a tank installed at several plants of one design class of plants a residual value of several centimetres was measured when the tank was empty. An alarm that should be triggered when the vessel is empty would not have been triggered. All of these events were complete CCFs.

7.3.7 Valves in wrong position

In four cases valves were in wrong positions (i.e., isolation valves closed and/or equalizer valves open) rendering the transmitter inoperable. All these events were events with at least two completely failed components (and Shared Cause Factor and Time Factor coded as "High"). In one event description it is stated that it is difficult to verify the position of the valves, and the valves had a history of operating errors. In another description it is stated that the valves were closed while the actuators were in the "open" position. The licensee had observed several problems with this type of valve. As an administrative measure, only personnel with specific training are allowed to operate these valves. For the valves of the components affected in a third event it was also difficult to verify the position of the valves.

7.4 ICDE events with long latent times

As mentioned before, the data set contains a relatively high share of events with long latent times (time from occurrence of failure to detection of failure). To understand the safety impact of these events an additional analysis was carried out. For (about 20%) of the events the latent time was one year/cycle or more. However, about half of these events were minor calibration errors in systems with test or maintenance intervals of one year or more. Affected signals were "Level 'Low' of steam generator secondary side" and "Level of accumulator". In these cases, test or maintenance practices were adequate to detect the impairments. The long latent times merely are a result of the long test or maintenance intervals.

In two other events minor calibration errors without safety significance were caused by an error when updating calibration data sheets of the accumulator level measurement.

Design errors in plant modifications caused two events with long latent times. In both events level measurement instruments had been replaced by devices with new technology. In one event, level switches of the reactor pressure vessel "Very low" level were replaced by a software based system. A calculation error of the theoretical calibration signal led to triggering the "Very low" signal at a level of 0.55 m lower than expected. This event is assessed as a complete CCF in the ICDE database.

In the second event depressurisation of the reactor was inadvertently triggered during a start up test after revision outage. In this outage instrumentation of the suppression pool level measurement was changed to a new technology in the second redundant train of the system. One year before, the same modification had been made in the first train. Only the failure in the first redundant train has a long latent time in this event as the first test after modification of the second redundant train revealed the design error. The third train of the system was not affected because the modification was not yet implemented.

Design and mounting errors at the time of plant construction led to the longest latent times in the analysed data set. Eight events belong to this group. In two of these events, latent time was more than ten years. A common feature of these events is that the affected signals are not triggered in normal operating conditions. The events can be characterised as follows:

- Wrong position of the sensors for the containment sump "Low" signal of the containment spray system would lead to triggering the signal at a sump level 0.4 m lower than expected.
- Wrong mounting position of the condensing chambers in the reference columns of the reactor pressure vessel level measurement would lead to a measurement error of up to 3 m of the reactor pressure vessel level in the long time phase of a LOCA. In normal operation and other LOCA situations the mismatch is less than (3%).

- Upper and lower pressure gauge lines of the accumulator “Low” level had been erroneously interchanged during plant construction at some (but not all) accumulators. Signal was permanently “High” for the affected accumulators.
- A design error of level “Low” nozzles of the containment spray tank led to never reaching level “Low” signal even when the tank was empty. These events are assessed as a complete CCF in the ICDE database.

In a further event five out of twelve transmitter isolation valves of the accumulator “Low” level measurement were left closed after revision outage. This was only detected in the next revision. In another event a false calibration of the pressuriser level transmitters due to erroneous data led to a wrong level indication which was too high by 0.6 m.

In conclusion, it can be stated that most of the events with long latent times have no or low safety significance. But, there are some events that may have a significant safety implication depending on plant specific behaviour in specific incident or accident situation. As the safety implication of the affected signals depends on individual plant design and event sequence it is not discussed in detail here.

A common feature of the observed events with long latent time is the impossibility of detection during power operation. The causes are either a common calibration error on redundant equipment preventing detection by comparison of redundant signals and/or that affected signals are not triggered since trigger values are not reached during power operation.

8. SUMMARY AND CONCLUSIONS

In summary, the CCF mechanisms present in most events reported do not pose a serious threat to the operability of safety systems. For Example, signal drifts of transmitters are usually discovered during transmitter tests or as conflicting level indications before a safety function is compromised. This is reflected in the coded component impairments; in most cases only incipient or degraded impairments were chosen.

However, some mechanisms observed pose a more serious threat to the availability of safety functions. This is usually related to the inability to test level measurement as a whole or to test it for all relevant liquid levels. Instead, only some parts, usually the transmitter is tested periodically in short time intervals. In some cases, even at plant commissioning, no full test had been carried out. Some features like the operability of condensation chambers under all relevant (e.g., accident) conditions cannot be tested at all.

To be able to discover CCF phenomena as early as possible and to avoid the occurrence of a CCF, it is essential to analyse systematically which parts of safety relevant level measurement are tested, which are testable and which are not testable.

If level measurement as a whole is not testable during operation, commissioning tests are of utmost importance and should be given great attention. In all tests, including recurrent tests, it is important to test level measurement as far as possible for all relevant liquid levels including verification that limit switches are triggered at correct levels. If a test as a whole is impossible, it should be analysed which possible errors are not covered by the tests that are carried out, e.g., incorrect valve positions, miscalculated setpoints. Regarding these aspects strategies should be developed to minimise the likelihood of errors and failures, e.g.,

- Isolation and equaliser valves should be ergonomic, i.e. they should be easy to operate and the position of the valves should be clearly identifiable, such that the likelihood of valves remaining in a wrong position after tests is minimised.
- A systematic approach should be established to ensure that after system modification relevant setpoint calculations and operation and test procedures are modified appropriately and that the use of outdated procedures is prevented. Interface problems between existing and new technologies should be given special attention.

9. REFERENCES

[1] NEA CSNI website, list of CSNI reports: http://www.nea.fr/html/nsd/docs/indexcsni.html and ICDE site http://www.nea.fr/html/jointproj/icde.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] Kreuser, A. Coding Guidelines for Level Measurement. ICDECG07 Draft 1.5, January 2006.

[5] 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.

APPENDIX A

Recommendations on Observed Population data and on CCF event descriptions resulting from ICDE Steering Group workshop on level measurement data exchange

Recommendations on observed populations

- Use the subcomponent feature of the database to build observed population records with different degrees of redundancy to describe the equipment for one system (i.e., a vessel in the level measurement database).

- The idea for grouping should be to include all equal equipment in one observed population. Examples:

  - All limit switches, even if connected to transmitters of different type.
  - Equal equipment for level measurement of several boilers or steam generators in one plant.
  - Identical equipment that belongs to two different shut down systems but both systems have the same function of level measurement for one vessel (with the only difference that it is maintained by different maintenance teams) should be in one group because there is no significant difference between the components.
  - If there are different numbers of sensors from pairs of gauge lines, define sensors in one observed population and gauge lines in another.
  - Transmitters of different types/technologies can be put in one observed population, but description should justify why.
  - Transmitters from different manufacturers but otherwise same type should be put in one observed population. The discriminating feature "manufacturer" can be considered in the PSA model.

- The degree of detail of the description in the observed population definition field G1 is essential to understand both the technology of the equipment and the grouping of the components. The description should explain the reasons for grouping components in one observed population. It is important to understand why components belong to one group.

- If a group of components is described on subcomponent level this should be mentioned in the G1 definition field. Mention also the related subcomponent group records. The relationship between subcomponents should be defined clearly.

- If more than one observed population is set up for one type of subcomponent in one system, the description in the G1 definition field should explain the difference between these observed populations (e.g., different function in the system).

- The field G8 (observed population number) can be used to distinguish records if several observed populations would have otherwise identical field G0 (observed population name).

- For very complex systems (e.g., level measurement of the BWR reactor pressure vessel and the BWR reactor scram tanks) a diagram may be needed to understand the relationship of the components. Such diagrams can be added to the level measurement component coding guide.

- If equipment was changed during the data collection period (e.g., redundancy, technology of the transmitters) it is reasonable to create two sets of observed populations. The definition in G1 benefits from up-front description of changes made.

- Information about scope of tests is needed to decide about: is time factor high or low for two failures which are separated by time. An explanation should be given in the definition field G1 about the test interval (surveillance test or more thorough test with longer time interval). The coded test interval should be the shortest interval.

- Abbreviations in descriptions should be explained.

Recommendations on CCF event descriptions

- If a CCF event affected components that belong to two observed populations then two event records should be made. Each event record should describe the observed impairments of the components of its corresponding observed population.
- In order to be able to validate the impairment coding the event description field C5 should contain information that explains the impairment coding. (e.g., the magnitude of deflection of a transmitter signal should be given if available.).
- Latent time (field C2-2) is put to zero for monitored failures only. If components are not permanently monitored but are checked regularly (e.g. on walkdowns), latent time is e.g. one day. It is possible that an event with latent time zero has a time factor "High" (e.g., multiple failures to run during mission time). Latent time can be larger than the shortest test interval (which is indicated in field G5-1 of the observed population record) if a failure cannot be detected in e.g., three monthly routine testing, but only in e.g., three yearly intensive testing. This should be explained in the event description field C5.
- It has to be recognised that for some events the information given is all information available from the original records but description may not be clear enough to understand e.g., the detection means or the degree of impairment.
- Root cause coded in field C9 is a high level classification. The value list of field C9 does not represent "real" root causes. These are only described in the event description field C5.
- If some but not all components failed in a system containing several vessels (e.g., steam generators) it matters to know whether the failures were on the same or on different vessels. This information may be important to know how to prevent or to protect.
- If not obvious, additional information is needed to understand the number of exposed components.
- If available, event description should mention the safety consequences of the observed failure to the component, e.g., if the signal deflection is to the high or low side.

If not obvious, event description should clarify reasoning for root cause coding, corrective action coding etc.

APPENDIX B

Table B.1 **Root cause distribution**

Root Cause	No. of events	Percentage
A – Abnormal environmental stress	5	3.4%
C – State of other component(s)	19	13.0%
D – Design, manufacture or construction inadequacy	18	12.3%
H – Human actions, plant staff	15	10.2%
I – Internal to component, piece part	4	2.7%
M – Maintenance	2	1.3%
O – Other	65	44.5%
P – Procedure inadequacy	12	8.2%
U – Unknown	6	4.1%
TOTAL	**146**	**100%**

Table B.2 **Corrective action distribution**

Corrective Actions	No. of events	Percentage
A – General administrative/procedure control	25	17.1%
B – Specific maintenance/operation practices	78	53.4%
C – Design modifications	6	4.1%
D – Diversity	6	4.1%
E – Functional/spatial separation	19	13.0%
F – Test and maintenance policies	3	2.1%
G – Fixing of component	7	4.8%
O – Other	2	1.4%
U – Unknown	-	0.0%
TOTAL	**146**	**100%**

Table B.3 **Detection method distribution**

Detection	No. of events	Percentage
DE – Demand event	1	0.7%
MA – Maintenance/Test	6	4.1%
MC – Monitoring in control room	10	6.8%
MW – Monitoring on walkdown	40	27.4%
TA – Test during annual overhaul	11	7.5%
TI – Test during operation	75	51.4%
TL – Test laboratory	-	0.0%
TU – Unscheduled test	3	2.1%
U – Unknown	-	0.0%
TOTAL	**146**	**100%**