Nuclear Safety
NEA/CSNI/R(2020)17
March 2024
www.oecd-nea.org

ICDE Project Report: Common-Cause Failures of Safety and Relief Valves

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CSNI/R(2020)17

Unclassified **English text only**

27 March 2024

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

ICDE Project Report: Common-Cause Failures of Safety and Relief Valves

This document is available in PDF format only.

JT03540415

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 38 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

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

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

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 34 countries: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czechia, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia (suspended), the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom and the United States. The European Commission and the International Atomic Energy Agency also take part in the work of the Agency.

The mission of the NEA is:

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

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

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

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS (CSNI)

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

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

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

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

Foreword

Common-cause failure (CCF) events can significantly impact the availability of safety systems of nuclear power plants. For this reason, several Nuclear Energy Agency (NEA) member countries initiated the International Common-cause Failure Data Exchange (ICDE) project in 1994. In 1997, the NEA Committee on the Safety of Nuclear Installations (CSNI) formally approved the carrying out of this project within the OECD/NEA framework; since then the project has successfully operated over eight consecutive terms (the current and ninth term being 2023-2026).

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

The objectives of the ICDE project are to:

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

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

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

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

- NEA (2000), “Collection and Analysis of Common-Cause Failure of Centrifugal Pumps”, www.oecd-nea.org/jcms/pl_16434.
- NEA (2001), “Collection and Analysis of Common-Cause Failure of Emergency Diesel Generators”, www.oecd-nea.org/jcms/pl_17470.

- NEA (2001), "Collection and Analysis of Common-Cause Failure of Motor-Operated Valves", www.oecd-nea.org/jcms/pl_17516.
- NEA (2002), "Collection and Analysis of Common-Cause Failure of Safety Valves and Relief Valves" , www.oecd-nea.org/jcms/pl_17748.
- NEA (2002), "Proceedings of ICDE Workshop on the Qualitative and Quantitative Use of ICDE Data", www.oecd-nea.org/jcms/pl_17508..
- NEA (2003), "Collection and Analysis of Common-Cause Failure of Check Valves", www.oecd-nea.org/jcms/pl_17948.
- NEA (2003), "Collection and Analysis of Common-Cause Failure of Batteries", www.oecd-nea.org/jcms/pl_17978.
- NEA (2008), "Collection and Analysis of Common-Cause Failure of Switching Devices and Circuit Breakers", www.oecd-nea.org/jcms/pl_18524.
- NEA (2008), "Collection and Analysis of Common-Cause Failure of Level Measurement Components", www.oecd-nea.org/jcms/pl_18568.
- NEA (2012), "ICDE General Coding Guidelines – Updated Version", www.oecd-nea.org/jcms/pl_19122.
- NEA (2013), "Collection and Analysis of Common-Cause Failure of Centrifugal Pumps", www.oecd-nea.org/jcms/pl_19250.
- NEA (2013), "Collection and Analysis of Common-Cause Failure of Control Rod Drive Assemblies", www.oecd-nea.org/jcms/pl_19274.
- NEA (2013), "Collection and Analysis of Common-Cause Failure Of Heat Exchangers", www.oecd-nea.org/jcms/pl_19648.
- NEA (2015), "ICDE Workshop - Collection and Analysis of Common-Cause Failures due to External Factors", www.oecd-nea.org/jcms/pl_19670.
- NEA (2017), "ICDE Workshop - Collection and Analysis of Emergency Diesel Generator Common-Cause Failures Impacting Entire Exposed Population", www.oecd-nea.org/jcms/pl_19784.
- NEA (2018), "Lessons Learnt from Common-Cause Failure of Emergency Diesel Generators in Nuclear Power Plants – A Report from the International Common-Cause Failure Data Exchange (ICDE) Project", www.oecd-nea.org/jcms/pl_19852.
- NEA (2019), "ICDE Project Report: Summary of Phase VII of the International Common-Cause Data Exchange Project", www.oecd-nea.org/jcms/pl_19902.
- NEA (2020), "ICDE Topical Report: Collection and Analysis of Common-Cause Failures due to Plant Modifications", www.oecd-nea.org/jcms/pl_36527.
- NEA (2022), "ICDE Topical Report: Provision against Common-Cause Failures by Improving Testing", www.oecd-nea.org/jcms/pl_75196.
- NEA (2022), "ICDE Topical Report: Collection and Analysis of Multi-Unit Common-Cause Failure Events", www.oecd-nea.org/jcms/pl_75202.
- NEA (2022), "ICDE Topical Report: Collection and Analysis of Intersystem Common-Cause Failure Events", www.oecd-nea.org/jcms/pl_69830.

This report was approved by the Committee on the Safety of Nuclear Installations on 3 December 2020 during its 68th session (NEA, 2020), and prepared for publication by the NEA Secretariat.

Acknowledgements

The following individuals have significantly contributed to the preparation of this report: Simon Wakter (ÅF), Gunnar Johanson (ÅF) and Mattias Håkansson (ÅF).

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

Table of contents

Tables

Figures

List of abbreviations and acronyms

CCF	Common-cause failure
SRV	Safety and relief valve
ICDE	International common-cause failure data exchange
IRS	Incident reporting system
I&C	Instrumentation and control
LOSP	Loss of off-site power
MCC	Motor control centre
M/T	Maintenance/test
OP	Observed population
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment

Organisations

ANVS	Autoriteit Nucleaire Veiligheid en Stralingsbescherming (Authority for Nuclear Safety and Radiation Protection, Netherlands)
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Consejo de Seguridad Nuclear (Nuclear Safety Council, Spain)
CSNI	Committee on the Safety of Nuclear Installations
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat (Swiss Federal Nuclear Safety Inspectorate, Switzerland)
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (Institute of Radiological Protection and Nuclear Safety, France)
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission (United States)
OECD	Organisation for Economic Co-operation and Development
ONR	Office for Nuclear Regulation (United Kingdom)
SSM	Strålsäkerhetsmyndigheten (Radiation Safety Authority, Sweden)
STUK	Säteilyturvakeskus (Finnish Centre for Radiation and Nuclear Safety, Finland)

Executive summary

This report documents a study performed on the topic of common-cause failure (CCF) events for safety and relief valves (SRVs). In October 2002, the ICDE project published a report summarising the collection and analysis of SRV CCF events. The report examined 149 collected events spanning a period from 1977 through 1999. Since that time, the ICDE project has continued the collection of SRV CCF events. The database now includes 271 events spanning a period from 1977 through 2015. Hence, an update of the 2002 study was performed and is documented in this report.

The objectives of this report are:

- to describe and examine the data profile for safety and relief valves;
- 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.

This study presents an overview of the entire SRV data set. The events were examined by tabulating the data and observing trends. Once trends were identified, individual events were reviewed to gain additional insight. The data includes root causes, coupling factors, observed population (OP) sizes, corrective actions, degrees of failure, affected subsystems and detection methods. Charts and tables are provided, presenting the event count for each of these event parameters.

The data in the report were collected according to the internal processes of the participating organisations and checked according to their internal quality assurance programmes. The event information provided by the participating organisations is analysed within the scope of the project; the event data are not changed unless the events undergo a review by the responsible national co-ordinator. In general, the root causes presented in the report are not based on a full scope formal root cause analysis.

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

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

- The vast majority (78%) of events was due to the failure mode “movement of valve/pilot valve impeded”. The next most frequent failure mode was “valve/pilot valve leaking” (12%).
- Although the share of events due to “deficiencies in operations” is slightly higher than that due to “deficiencies in design, construction and manufacturing”, the latter has a slightly higher share for the more severe events.
- The causes for the more severe “design” events are predominantly linked to ageing, which could mean that shortened maintenance intervals or changes to the design and material are likely to help mitigate such issues.

- For the deficiencies in operations, the complete CCF events show strong indications of deficiencies in safety culture and training. For example, there were multiple events where maintenance activities were carried out on the wrong valves, valves were disabled (or put into manual mode), tests were carried out under the wrong plant conditions and equipment installed for test purposes was not removed after completion of the test.

1. Introduction

This report presents an overview of the exchange of common-cause failure (CCF) data of safety and relief valves (SRVs) among several countries. The objectives of this report are:

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

Section 2 presents a description of the safety and relief valve component. Section 3 presents an overview of the contents of the SRV database and a summary of statistics. Section 4 contains some high level engineering insights about the SRV CCF events. These insights are based on failure causes and failure mechanisms. Section 5 provides a summary and conclusions. References are found at the end of the report before the annexes.

The ICDE project was organised to exchange CCF data among participating countries. A brief description of the project, its objectives and the participating countries is given in Annex A. Annex B presents the definition of common-cause failures and the ICDE event definitions. Annexes C to E provide the failure analysis assessments, including a short description of each SRV event, the history of the events and the influences leading to the given failure ("the failure mechanism").

2. Component description

This section is based on safety and relief valve (SRV) coding guidelines, which are an appendix to the ICDE general coding guidelines (NEA, 2011).

2.1. General description of the component

The function of the safety valves/relief valves (SVs/RVs) is to prevent overpressure of the components and system piping. The systems for which SVs/RVs are installed in and data are collected for are (the corresponding IRS system coding is added in parentheses):

- Steam generator discharge headers, PWR (pressurised water reactor), AGR (advanced gas reactor), Magnox (3.AH).
- Pressuriser vapour volume, PWR (3.AF).
- Reactor coolant system, main steam headers, BWR (boiling water reactor), AGR, Magnox (3.BH)42.

The safety valve/relief valve component types are the following:

- Pressuriser power operated relief valves (PWR).
- Pressuriser safety valves (PWR).
- Steam generator power operated relief valves (PWR, AGR, Magnox).
- Steam generator safety valves (PWR, AGR, Magnox).
- Power operated relief valves (PWR, AGR, Magnox).
- ADS (automatic depressurisation system) valves (BWR).
- Primary-Side safety valves (BWR, AGR, Magnox).

2.2. Component boundaries

The component boundary in this data analysis includes the following: local instrumentation, control equipment, power contactors and other component parts specific to the valve. Functional modules for the main steam header SV/RV are exemplified in Figure 2.1. The function can be combined and therefore the following, optional, component sub-types for detailed classification are available.

A. Impulse operated valve (safety, relief, closing)

A.1 Main valve

A.2 Pilot valve

A.2a Impulse or spring-operated pilot valve

A.2b Electromagnetic pilot valve

A.2c Pneumatic pilot valve

A.2d Motor-operated pilot valve

B Spring- operated safety valve

C Motor-operated safety/relief valve

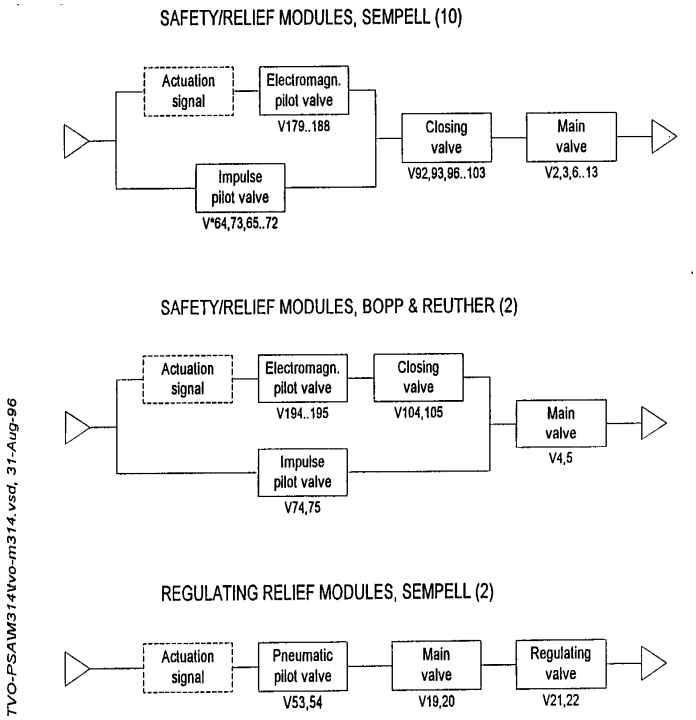
D Electromagnetic operated safety/relief valve

E Pneumatic operated safety/relief valve

2.3. Event boundary

Successful operation of a SV/RV is defined as the valve opening when system pressure exceeds a predefined threshold, and closing again when pressure is reduced below a predefined threshold. Note that the opening of SVs/RVs in response to an actual system overpressure is not a failure. Subsequent failures to re-seat completely are defined as a failure to close event.

Figure 2.1. Functional modules for main steam header safety and relief valves.



Source: NEA, 2011.

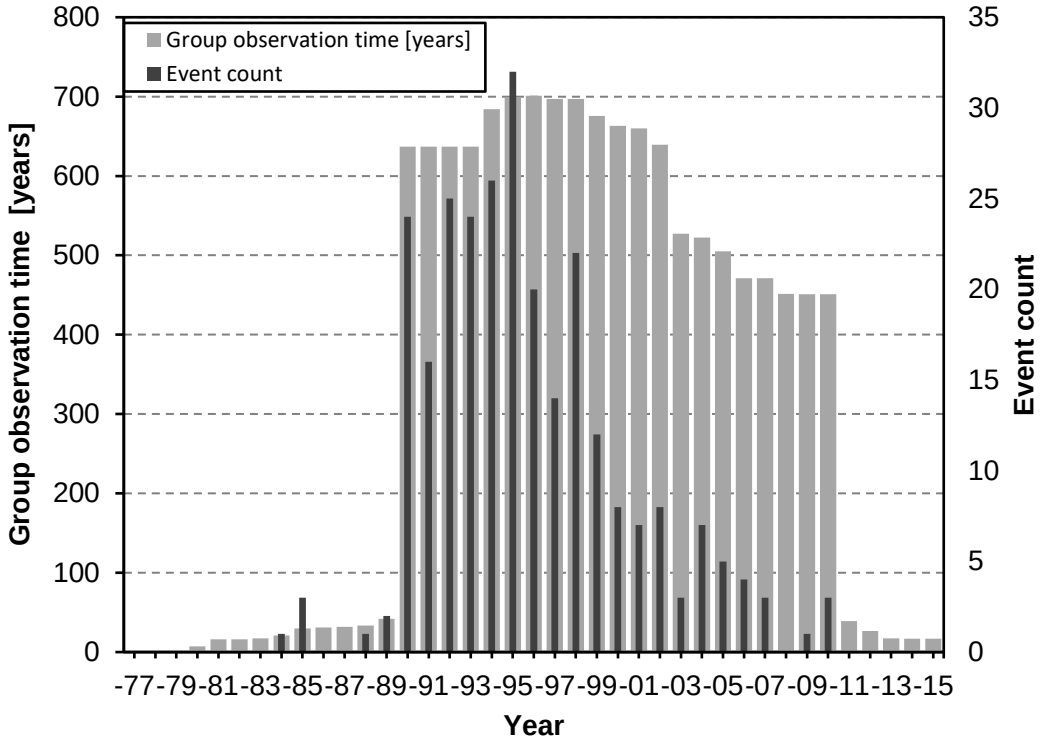
3. Overview of database content

3.1. Overview

CCF data have been collected for safety and relief valves. Organisations from Canada, Finland, France, Germany, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States have contributed to this data exchange. In all, 271 ICDE events were reported from nuclear power plants (pressurised water reactors, boiling water reactors, Magnox and advanced gas reactors) and the data span a period from 1977 through 2015. The data are not necessarily complete for each country throughout this period. Compared with the data covered by the previously published SRV report (NEA, 2022), 122 new events are covered in this report.

The data collection includes 229 reactor units and 12 861 group observation years. Figure 3.1 presents the data collection of group observation times (years) and number of events distributed over time.

Figure 3.1. Data collection: Group observation time and event count distribution over time.



The collection of these events has included both top-down work by identifying events on the basis of licensee event reports and bottom-up work by going through events in plant maintenance databases. Although most CCF events are identified through the former mechanism, the latter has led to ICDE events that were not identified otherwise. This bottom-up work is rather resource intensive.

The distributions of events in the following section is strictly based on the classes given in the ICDE coding guidelines (NEA, 2011) and as coded by the national co-ordinators. The root causes presented here are in general not based on a full scope formal root cause analysis. In Section 4, a deeper engineering analysis of the events is presented.

3.2. Failure mode and impact of failure

Malfunctions of SRVs are defined in the safety and relief valve coding guidelines (NEA, 2011) as failures to open or close on demand; failure to stay closed, including excessive leakage through the valve; and spurious opening of the valve. The failure modes used in evaluating the data are:

- **Failure to open (FO):** for example, when an SRV is stuck closed or whenever a SRV is blocked shut.
- **Failure to close (FC):** for example, an SRV stays open when it should close or it doesn't fully close.
- **Inadvertent opening (IO):** for example, a spurious opening, leakage past the valve seats, and a piece-part(s) being replaced to re-calibrate a set point that was too low.

Some countries also use the following failure modes:

- **Internal leakage (IL).**
- **Spurious operation (SO).** This code may be used, for example, for a failure to stay open.
- **Others (O).**

For each event in the ICDE database, the impairment of each component in the observed population (OP) has been defined according to the categorisation in the General Coding Guidelines (NEA, 2011):

- **C** denotes complete failure. The component has completely failed and will not perform its function. For example, if the cause prevents an SRV from opening, the SRV has completely failed and impairment would be complete. If the description is vague, this code is assigned in order to be conservative.
- **D** denotes degradation. The component is capable of performing the major portion of the safety function, but parts of it are degraded. For example, a valve not opening fully or taking too long to open or close.
- **I** denotes incipient degradation. 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 a working component, i.e. it has suffered no damage and is working according to specifications.

The degree of severity is indicated by the severity category, as defined by the ICDE General Coding Guidelines (NEA, 2011). The different severity categories are:

a) Complete CCF = All components in the group are completely failed (i.e. all elements in impairment vector are C, time factor high and shared cause factor high).

b) Partial CCF = At least two components in the Group are completely failed (i.e. time factor high and shared cause factor high and at least two C in the impairment vector, but not complete CCF).

c) CCF Impaired = At least one component in the group is completely failed and others affected (i.e. at least one C and at least one I or one D in the impairment vector, but not partial CCF or complete CCF).

d) Complete impairment = All components in the exposed population are affected, no complete failures but complete impairment. Only incipient degraded or degraded components (all D and/or I in the impairment vector).

e) Incipient impairment = Multiple impairments but at least one component working. No complete failure. Incomplete but multiple impairments with no C in the impairment vector.

f) Single impairment = the event does not contain multiple impairments. Only one component impaired. No CCF event.

g) No impairment = All components working or no impairment data given.

Table 3.1 and Figure 3.2 show the distribution of the events by failure mode and severity category. Figure 3.3 shows the percentages of events in each severity category out of the total event count for each failure mode. The most dominant severity categories are the least severe, complete impairment (d) and incipient impairment (e).

The most common failure mode, with 71% of the total events count, was *failure to open* (FO). A total of 26 events (10%) were complete CCF (a) events, meaning all components in the exposed population failed completely due to the same cause and within a short time interval. No severity category (g), no impairment, events are included in the data.

Table 3.1. Distribution of severity per failure mode

Failure mode	a	b	c	d	e	f	g	Event count
Failure to Open (FO)	21	28	23	59	61			192
Failure to Close (FC)	4	5	5	9	15	1		39
Inadvertent Opening (IO)		3	4	13	8			28
Internal Leakage (IL)	1		1	3	2			7
Spurious Operation (SO)				1				1
Others (O)				3	1			4
Total event count	26	36	33	88	87	1		271

Figure 3.2. Distribution of severity category per failure mode.

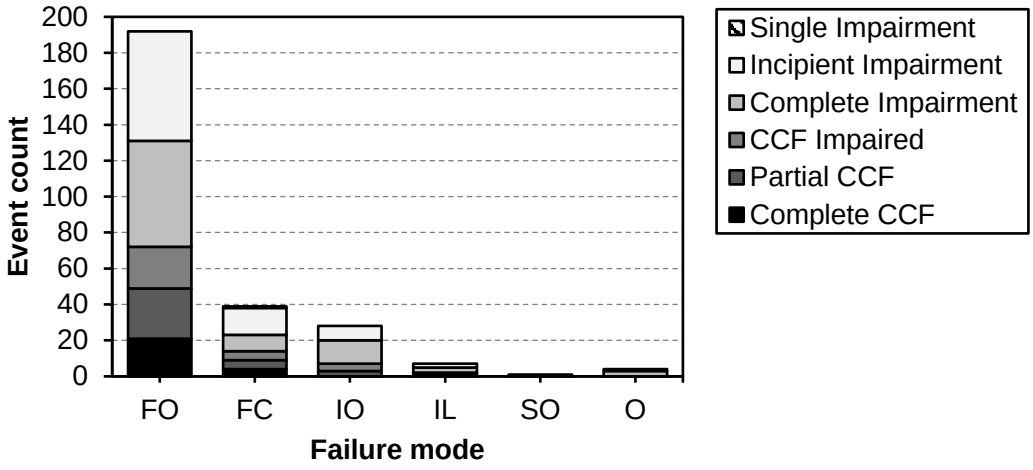
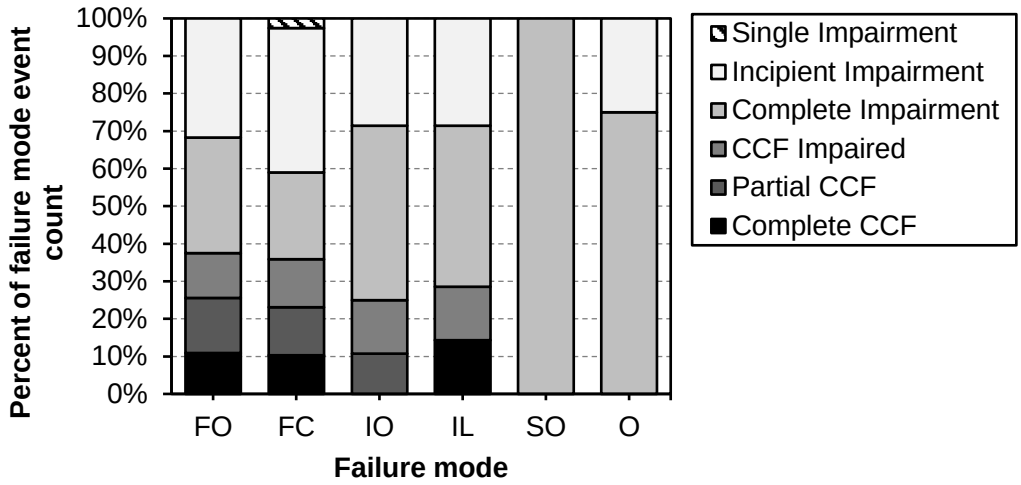


Figure 3.3. Distribution of severity category as percentages for each failure mode event count



3.3. Event cause

In the ICDE database the event cause describes the direct reason for the component's failure. For this project, the appropriate code is the one representing the common-cause, or if all levels of causes are common-cause, the most readily identifiable cause. The following coding was suggested:

C **State of other components.** The cause of the state of the component under consideration is due to the state of another component.

D **Design, manufacture or construction inadequacy.** This category encompasses actions and decisions taken during the design, manufacture or installation of components, both before and after the plant is operational. Included in the design process are the equipment and system specification, material specification and initial construction that would not be considered a maintenance function. This category also includes design modifications.

A **Abnormal environmental stress.** This represents causes related to a harsh environment that is not within component design specifications. Specific mechanisms include chemical reactions, electromagnetic interference, fire/smoke, impact loads, moisture, radiation, abnormally high or low temperature, vibration load and severe natural events.

H **Human actions.** This represents causes related to errors of omission or commission on the part of plant staff or contractor staff. This category includes accidental actions and failure to follow procedures for construction, modification, operation, maintenance, calibration and testing. This category also includes deficient training.

M **Maintenance.** All maintenance not captured by H – human actions or P – procedure inadequacy.

I **Internal to component or piece-part.** This deals with malfunctioning of internal parts to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the environment on the component. Specific mechanisms include corrosion/erosion, internal contamination, fatigue and wear out/end of life.

P **Procedure inadequacy.** Refers to ambiguity, incompleteness or error in procedures for the operation and maintenance of equipment. This includes inadequacy in construction, modification, administrative, operational, maintenance, test and calibration procedures. This can also include administrative control procedures such as change control.

O **Other.** The cause of the event is known, but does not fit in one of the other categories.

U **Unknown.** This category is used when the cause of the component state cannot be identified.

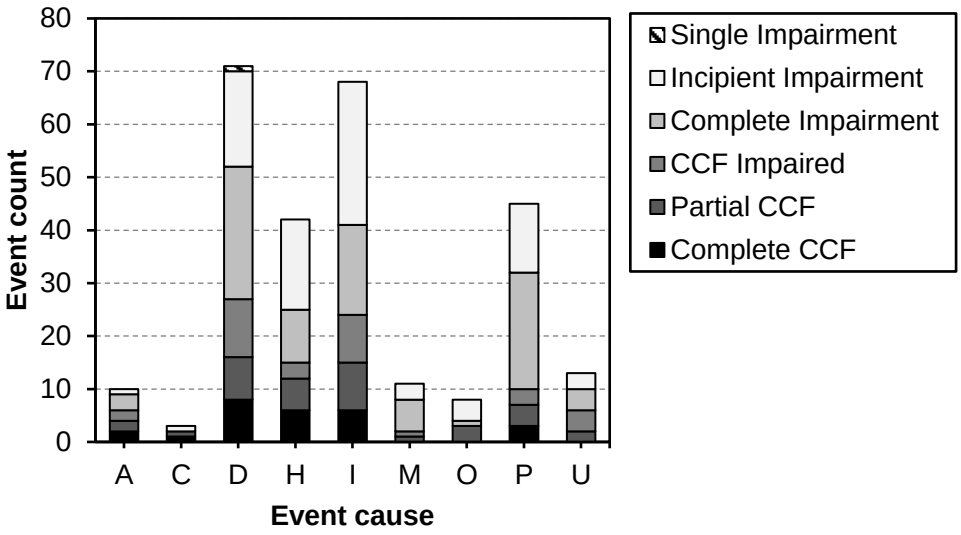
Table 3.2 and Figure 3.4 show the distribution of the events by event cause[1]. The primary event cause is *design manufacture or construction inadequacy* (D) closely followed by the event cause *internal to component or piece-part* (I), accounting for 26% and 25% of all failure events, respectively.

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

Table 3.2. Distribution of event cause per severity category

Event Cause		Severity category a	b	c	d	e	f	g	Event count
Abnormal environmental stress	(A)	2	2	2	3	1			10
State of other component(s)	(C)	1	1			1			3
Design, manufacture or construction inadequacy	(D)	8	8	11	25	18	1		71
Human actions, plant staff	(H)	6	6	3	10	17			42
Internal to component or piece-part	(I)	6	9	9	17	27			68
Maintenance	(M)		1	1	6	3			11
Procedure inadequacy	(P)		3		1	4			8
Other	(O)	3	4	3	22	13			45
Unknown	(U)		2	4	4	3			13
Total event count		26	36	33	88	87	1	0	271

Figure 3.4. Distribution of event cause for SRV events presented in a stacked chart by severity category



3.4. Coupling factors

The ICDE general coding guidelines (NEA, 2011) 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 event cause and the coupling factor are broadly similar, with the combination of coding serving to give more detail as to the causal mechanisms.

Selection is made from the following codes:

H Hardware (component, system configuration, manufacturing quality, installation, configuration quality). Coded if none of or more than one of HC, HS or HQ applies, or if there is not enough information to identify the specific "hardware" coupling factor.

HC Hardware design. Components share the same design and internal parts.

HS System design. The CCF event is the result of design features within the system in which the components are located.

HQ Hardware quality deficiency. Components share hardware quality deficiencies from the manufacturing process. Components share installation or construction features from initial installation, construction or subsequent modifications

O Operational (maintenance/test (M/T) schedule, M/T procedures, M/T staff, operation procedure, operation staff). Coded if none or more than one of OMS, OMP, OMF, OP or OF applies, or if there is not enough information to identify the specific "maintenance or operation" coupling factor.

OMS M/T schedule. Components share maintenance and test schedules. For example, the component failed because a maintenance procedure was delayed until failure.

OMP M/T procedure. Components are affected by the same inadequate maintenance or test procedure. For example, the component failed because the maintenance procedure was incorrect or the calibration set point was incorrectly specified.

OMF M/T staff. Components are affected by maintenance staff error.

OP Operation procedure. Components are affected by inadequate operations procedure.

OF Operation staff. Components are affected by the same operations staff personnel error.

E Environmental, internal and external.

EI Environmental internal. Components share the same internal environment. For example, the process fluid flowing through the component was too hot.

EE Environmental external. Components share the same external environment. For example, the room that contains the components was too hot.

U Unknown. Sufficient information was not available in the event report to determine a definitive coupling factor.

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

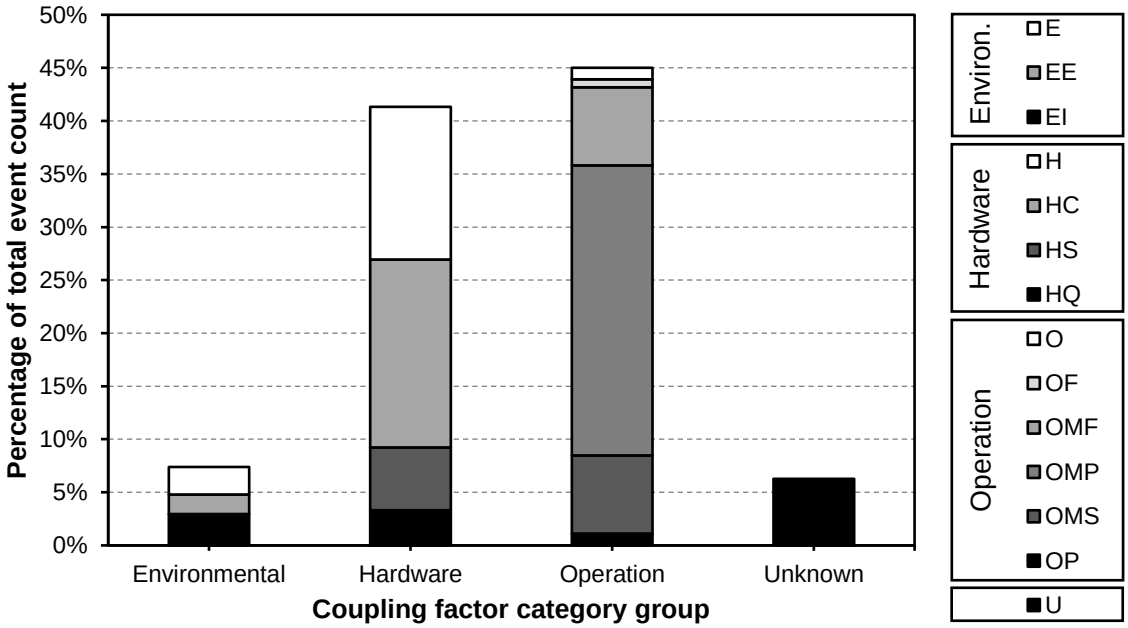
- Environmental: E, EE, EI.
- Hardware: H, HC, HS, HQ.
- Operation: O, OMF, OMP, OP, OF, OMS.

Table 3.3 and Figure 3.5 show the distribution of the events by coupling factor. A total of six events have not been assigned a coupling factor category (no data) and are therefore presented in the category *unknown*. The dominant coupling factor category group is *operation*, which accounts for 45% of the SRV events. Out of the 122 events in this category, 74 are due to deficiencies in maintenance and testing procedures (category code *OMP*). The second most prominent coupling factor category is *hardware*, which accounts for 41% of the SRV events. In the *hardware* category, the most common coupling factor is *hardware design* (HC) with 48 events.

Table 3.3. Distribution of coupling factors per severity category

	Severity category							
Coupling factor category	a	b	c	d	e	f	g	Event count
Environmental		7	5	5	3			20
Hardware	15	15	12	29	40	1		112
Operation	10	11	11	49	41			122
Unknown	1	3	5	5	3			17
Total event count	26	36	33	88	87	1	0	271

Figure 3.5. Distribution of SRV event coupling factors



3.5. Detection method

The ICDE general coding guidelines (NEA, 2011) suggest the following coding for the detection method for each failed component of the exposed population:

MW monitoring on walkdown

MC monitoring in control room

MA maintenance/test

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

TI test during operation

TA test during annual overhaul

TL test during laboratory

TU unscheduled test

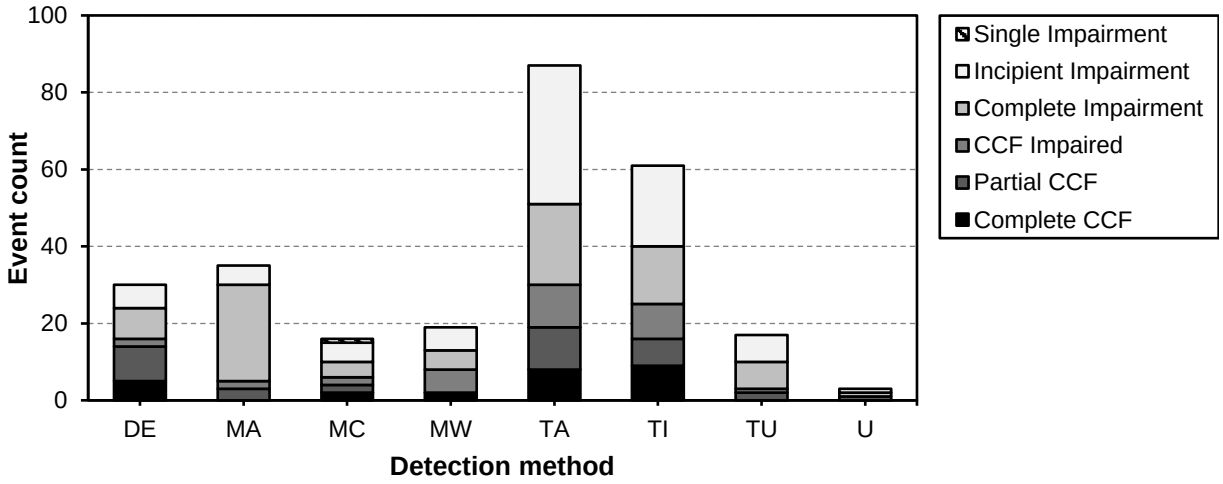
U unknown

The distribution of events by detection method is shown in Table 3.4 and Figure 3.6. Three events were excluded from the analysis because it was not possible to determine the detection method at the time of the analysis. Three events were coded as detection method *unknown (U)*, where the detection method is known but does not fit one of the existing detection method codes. The vast majority (148 events or 55% of total) were discovered through testing, either through *test during annual overhaul (TA)* (87 events, or 32% of total) or through *test during operation (TI)* (61 events or 23% of total). A minority of events (30, or 11% of total) are *demand events (DE)* but a disproportionally large amount of these events are complete CCFs or partial CCFs, making up 19% and 26% of those events, respectively.

Table 3.4. Distribution of detection methods per severity category

Detection method	Severity category							Event count
	a	b	c	d	e	f	g	
Demand event (DE)	5	9	2	8	6			30
Maintenance/test (MA)		3	2	25	5			35
Monitoring in control room (MC)	2	2	2	4	5	1		16
Monitoring on walkdown (MW)	2		6	5	6			19
Test during annual overhaul (TA)	8	11	11	21	36			87
Test during operation (TI)	9	7	9	15	21			61
Unscheduled test (TU)		2	1	7	7			17
Unknown (U)		1		1	1			3
Event count total	26	35	33	86	87	1	0	268

Figure 3.6. Distribution of SRV event detection methods



3.6. Corrective actions

The ICDE general coding guidelines (NEA, 2011) 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 event cause and/or coupling factor between the impairments". The following coding is suggested:

A - general administrative/procedure controls

B - specific maintenance/operation practices

C - design modifications

D - diversity

E - functional/spatial separation

F - test and maintenance policies

G - fixing of component

O - other

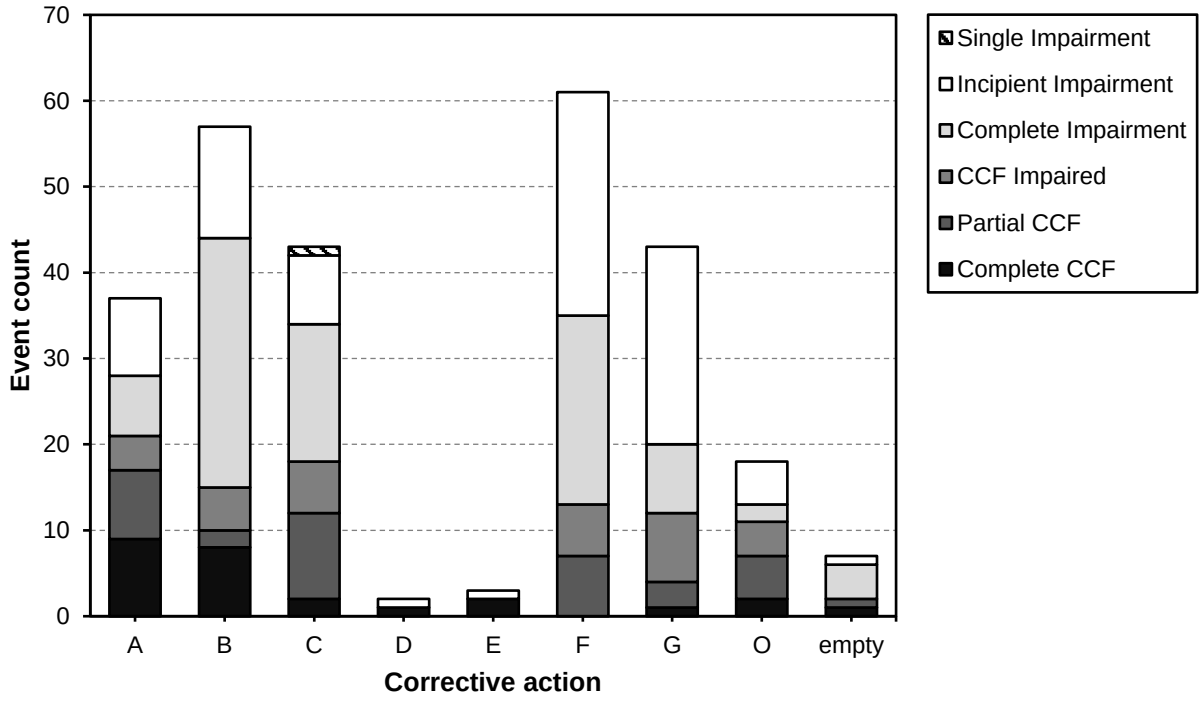
U - unknown (No data)

The distribution of events by corrective action is shown in Table 3.5 and Figure 3.7. Almost half, 43%, of all events, are corrected through maintenance actions, either through *test and maintenance policies (F)* (61 events, or 22.5% of total events) or through *specific maintenance/operation practices (B)* (57 events, or 21% of total events). For complete CCF events, the most common corrective actions taken are *general administrative/procedure controls (A)* (nine events, or 35% of complete CCF events) and *specific maintenance/operation practices (B)* (eight events, or 31% of complete CCF events).

Table 3.5. Distribution of corrective actions per severity category

	Severity category							
Corrective action	a	b	c	d	e	f	g	Event count
General administrative/ procedure controls (A)	9	8	4	7	9			37
Specific maintenance/ operation practices (B)	8	2	5	29	13			57
Design modifications (C)	2	10	6	16	8	1		43
Diversity (D)	1				1			2
Functional/spatial separation (E)	2				1			3
Test and maintenance policies (F)		7	6	22	26			61
Fixing of component (G)	1	3	8	8	23			43
Other (O)	2	5	4	2	5			18
No Data (empty)	1	1		4	1			7
Total event count	26	36	33	88	87	1	0	271

Figure 3.7. Distribution of SRV event corrective actions



4. Engineering aspects of the collected events

4.1. Assessment basis

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

Failure mechanism description

The failure mechanism is a history describing the observed events and influences leading to a given failure. Elements of the failure mechanism could be a deviation or degradation or a chain of consequences. It is derived from the event description and should preferably consist of one sentence.

Failure mechanism category

A failure mechanism sub-category encompasses component-type-specific observed faults or non-conformities that have led to the ICDE event. A failure mechanism category is a group of similar failure mechanism sub-categories. Table 4.1 presents the failure mechanism categories and their sub-categories for SRV.

Table 4.1. Failure mechanism categories and sub-categories

Failure mechanism category		Failure mechanism sub-category	
SRV-FM1	Movement of valve/pilot valve impeded	SRV-a1	Deposits of dirt or oxidation products
		SRV-a2	Missing or degraded lubrication
		SRV-a3	Scratched or degraded seat/disk/O-ring/seal surfaces
		SRV-a4	Bonding
		SRV-a5	Misalignment of switches, disk or in valve settings
		SRV-a6	Wrong set point of limit switch, torque switch misadjustment
		SRV-a7	I&C or actuator equipment failure
		SRV-a8	Loose/broken/degraded screws, bolts, hinges, bushings, pistons, diaphragms, springs
SRV-FM2	Valve/pilot valve leaking	SRV-b1	Valve leaking due to seat/disk/O-ring/seal surface degradation
SRV-FM3	Others	SRV-c1	H_2 build-up
		SRV-c2	Other/unknown

Failure cause category

The codes for failure causes are not component-dependent; however, they are dependent on the root cause and coupling factors. By definition, it is the coupling factor that identifies the mechanism that ties together multiple failures and the influences that created the conditions for multiple components to be affected. The root cause alone does not provide the information required for identifying failure cause categories. The failure cause categories are distributed over two types of groups, deficiencies in operation and deficiencies in design, construction and manufacturing:

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

Marking of interesting events

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

4.2. Failure analysis assessment matrix

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

The most common type of failure mechanism among all observed SRV events is FM1, movement of valve/pilot valve impeded (78% of events). The failure mechanism of the remaining events is roughly equally split between FM2, valve/pilot valve leaking, (12% of events) and others (10% of events).

The failure mechanisms are further broken down into sub-categories, see Table 4.1 and Table 4.3. The three most common failure mechanism sub-categories, constituting 46% of all events, are:

- wrong set point of limit switch, torque switch maladjustment (21% of events);
- loose/broken/degraded screws, bolts, hinges, bushings, pistons, diaphragms, springs (19% of events);
- I&C or actuator equipment failure (15% of events).

The failure causes of the SRV events are roughly equally divided between deficiencies in operation (52% of events) and deficiencies in design, construction and manufacturing (42% of events), see Table 4.2. Failure cause category D, deficiency in design of hardware, and category O1, deficient procedures for maintenance and/or testing, are the two most common (both with 37% of events). The two failure cause categories D and O1 also make up the vast majority of events within deficiencies in design, construction and manufacturing and deficiencies in operation, constituting 77% and 70% of events within each respective group. Seventeen events did not fit an existing description and so are identified as U, unknown.

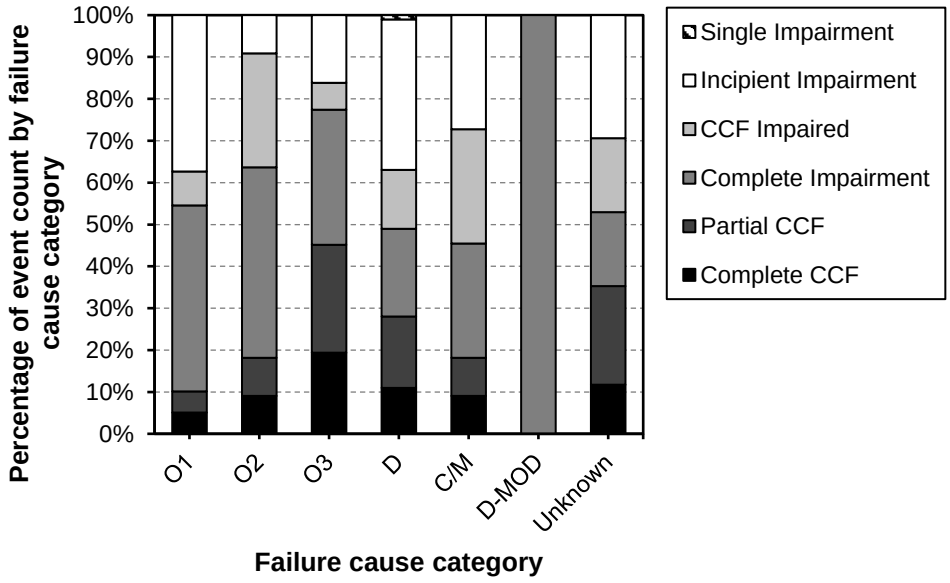
Table 4.2. Failure analysis assessment matrix

	Failure mechanism category			
Failure cause categories	FM1 Movement of valve/pilot valve impeded	FM2 Valve/pilot valve leaking	FM3 Others	Total
Deficiencies in operation	**119**	**14**	**8**	**141**
O1	82	13	4	99
O2	10	1	0	11
O3	27	0	4	31
Deficiencies in design, construction, manufacturing	**88**	**18**	**7**	**113**
D	75	18	7	100
C/M	11	0	0	11
D-MOD	2	0	0	2
Unknown	**5**	**1**	**11**	**17**
Total	**212**	**33**	**26**	**271**

Table 4.3. Failure analysis assessment matrix with failure mechanism sub-categories

Failure cause categories	Failure mechanism category and sub-category											
	FM1 Movement of valve/pilot valve impeded								FM2 Valve/pilot valve leaking	FM3 Others		
	a1	a2	a3	a4	a5	a6	a7	a8	b1	c1	c2	Total
Deficiencies in operation												
O1	3	6	5	1	8	44	3	12	13	0	4	99
O2	0	0	0	0	0	0	7	3	1	0	0	11
O3	1	1	0	1	10	6	6	2	0	0	4	31
Deficiencies in design, construction, manufacturing												
D	13	0	2	11	0	6	19	24	18	4	3	100
C/M	0	0	0	1	0	0	2	8	0	0	0	11
D-MOD	0	0	0	0	0	0	1	1	0	0	0	2
Unknown	**0**	**0**	**0**	**1**	**1**	**0**	**2**	**1**	**1**	**0**	**11**	**17**
Total	**17**	**7**	**7**	**15**	**19**	**56**	**40**	**51**	**33**	**4**	**22**	**271**

Figure 4.1. Percentage of events by event severity and failure cause category



4.3. Failure analysis assessment of deficiencies in operation

The most common failure cause category for events caused by deficiencies in operation is category O1, deficient procedures for maintenance and/or testing, followed by O3, insufficient qualification and/or work control during maintenance/test or operation, see Table 4.2. Figure 4.1 shows the share of events by event severity for each failure cause category.

This section presents an overview of each failure cause category related to deficiencies in operation.

Deficient procedures for maintenance and/or testing (O1)

Out of the 99 events identified with failure cause category O1, five events are complete CCFs. The share of high severity events is lower when compared to the other categories with deficiencies in operation, see Figure 4.1.

The largest single group of events overall consists of events with failure mechanism a6, wrong set point of limit switch, torque switch maladjustment, and failure cause O1 (44 events, 16% of events). Three events are complete CCFs and this group alone makes up almost half of all events in failure cause category O1. Two of the CCFs are linked to the incorrect computation resulting from using incorrect measurements. The event was a multi-unit event as it affected two different reactors of the same type.

The procedure deficiencies in these events often relate to calculation errors, e.g. of the seat area, scaling factor or calculation errors due to incorrect vendor data. Other events can be linked to failure to update the maintenance procedures. There are also calibration errors due to the improper use of calibration benches or incorrect measurements of valve lift. Some testing errors were linked to an inadequate testing method. Finally, the failure in some events to follow procedures was linked to poor or insufficient training. There were also events with no known cause, e.g. the incorrect settings of torque limit switches or set point drift occurring without a clearly identified cause.

Two more groups, with failure mechanism sub-category b1, valve leakage, (13 events, 5% of events) and sub-category a8, loose and degraded parts, (12 events, 4% of events), make up a further 25% of the events identified with failure cause O1.

There were no complete or partial CCFs identified for the b1/O1 events and overall only a single actual component failure, with the rest being impairments. It was not possible to determine any apparent cause for the failure, nor was it possible to determine any overall recommendations for this group as a whole. Six out of the thirteen events were repeating events (three events repeating once) from the same plant, which could be interpreted as a possible deficiency in safety culture.

Two out of twelve events identified as a8/O1 were complete CCFs and one event was a partial CCF. All three events with a high severity involved problems with the diaphragm, which was installed incorrectly for both complete CFF events. The coupling factor for all events was maintenance-related.

A further eight events were identified with failure mechanism a5, misalignment of switches, disk or in valve settings. These events were less severe than other events. A possible reason is that the relief valve stays operational but in a degraded state. However, all events involved complete impairment across large group sizes and the time factor was high for all events.

It was not possible to develop any further insights from the other failure mechanism sub-categories with failure cause category O1 beyond establishing the failure mechanism sub-category itself.

Insufficient attention to ageing of piece parts (O2)

Eleven events were identified with failure cause O2. One event with failure mechanism a7, I&C or actuator equipment failure, was a complete CCF. Another event with failure mechanism a8, loose/broken/degraded parts, was a partial CCF. For both of these events,

high temperatures contributed to faster than expected ageing of the components and the corrective action taken related to administrative/procedure protocols.

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

There were 31 events with failure cause O3. Six of those were complete CCFs, and eight events were partial CCFs. This means that almost half of the events with failure cause O3 were high severity events, which is the highest proportion out of the three failure cause categories related to deficiencies in operation, see Figure 8.

The largest group is the group identified with failure mechanism a5, misalignment of switches, disks or valve settings, with ten events. Out of these ten, four were complete CCFs and three were partial CCFs. Common issues were identified as failure to follow established procedures, in combination with a failure to detect this between different components. The complete CCF events show strong indications of deficiencies in safety culture and training. For example, there were multiple events where maintenance activities were carried out on the wrong valves, valves were disabled (or in manual mode), tests were carried out under the wrong plant conditions and equipment installed for test purposes was not removed after completion of the test.

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

	Failure mechanism category		
Failure cause categories	Movement of valve/pilot valve impeded	Valve/pilot valve leaking	Others
Deficiencies in operation	**119**	**14**	**8**
O1	Many of the events (44/82) relate to wrong set point or torque switch misadjustment (a6). Other events related to loose and degraded piece parts (12/82, a8), especially of the diaphragm for high severity events. Most events seem strongly linked to inadequate procedures or inadequate training. (82)	There is only one sub-category for this failure mechanism (13/13, b1). Low severity for all events. Six events are repeating events, which possibly shows deficiencies in safety culture. (13)	Problems relate to inadequate testing procedures or testing conditions. No failure mechanism (c2), in one case because there was no failure (only incipient). (4)
O2	Most events (7/10) relate to I&C or actuator problems (a7). One such event was a complete CCF. The rest related to loose piece parts (3/10, a8). For many events from both categories the common aspect was accelerated ageing from high temperature environments. (10)	O-ring became brittle which led to air leaks, (b1, 1/1 events). (1)	-
O3	Failure to adhere to procedures, either due to inadequate training or inadequate procedures resulted in a large share of high severity events. Many events (10/27) related to incorrect installation, misalignment and disabling of components (a5). Other events related to wrong set point (6/27, a6) as well as I&C and actuator problems (6/27, a7). Strong safety culture aspects. (27)	-	Operator error resulted in tests conducted at wrong conditions or on wrong components led to disabled components (4/4, c2). Strong safety culture aspects. (4)

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

The most common cause (77%) of the events caused by deficiencies in design, construction and manufacturing is failure cause category D, deficiency in design of hardware (100 events, 37% of all events). A further 11 events are identified as C/M, deficiency in construction or manufacturing of hardware. Figure 4.1 shows the share of events by event severity for each failure cause category.

This section presents an overview of each failure cause category related to deficiencies in design, construction and manufacturing.

Deficiency in design of hardware (D)

Out of the 100 events identified as failure cause category D, 11 events are complete CCFs. The share of high severity events is relatively high when compared with other failure cause categories, see Figure 4.1.

The largest single group consists of events identified with failure mechanism a8, loose and degraded piece parts (24 events, 9% of events). Three of those events are complete CCFs and two events are partial CCFs. Two of the complete CCF events and both partial CCF events are linked to problems with the diaphragms. In total, 17 out of 24 events are linked to diaphragms. Ageing effects were commonly observed on the diaphragms together with loose bolts, possibly as a secondary effect, leading to air leakage. One valve was affected by hydrogen-induced stress-corrosion cracking. The diaphragms seem to suffer from ageing (due to temperatures) which could mean that updated and shortened maintenance intervals or changes to the design and material are likely to help mitigate such issues.

The geographical and temporal spread (for 15 out of 24 events) indicates that it could potentially be a localised issue. No correlation between event severity and common failure aspects was observed.

The second largest group consists of events identified as a7, I&C or actuator equipment failure (19 events, 7% of events). There are six complete CCFs and five partial CCFs, and so a relatively large proportion of high severity events in this group.

Two complete CCFs involved failure of the valve actuator, one possibly due to ageing and the other resulting from a design error resulting in the opening force being too small. The other four complete CCF events all involved failure of electrical I&C components, meaning failure of switches and fuses. At least one event resulted from two valves sharing a common fuse that had failed.

Despite most events being clearly linked to deficiencies in design, there was only one event for which the corrective action was design modifications. Most corrective actions involved procedural changes, surveillance and administrative changes.

The third most common group includes events identified as b1, valve leakage (18 events, 7% of events). There is one complete CCF and one partial CCF in this group. The common failure between all of these events was established as inadvertent opening or leakage caused by different failure mechanisms. These include relaxation of the spring, vibration and corrosion but it was not possible to establish a general failure mechanism. For example, several causes of corrosion were observed, including flow-assisted corrosion near transitions between different materials, chloride induced stress-corrosion and corrosion at welds between ferritic and austenitic steel.

The majority of the remaining events were identified as either a1, deposits of dirt or oxidation products (13 events, 5% of events), or a4, bonding (11 events, 4% of events). Three events identified as a1/D are partial CCFs. One event identified as a4/D is a complete CCF and three events are partial CCFs.

Both groups (a1/D and a4/D) were affected by corrosion, bonding and sticking caused by inappropriate material combinations (e.g. metallurgical bonding) or inappropriate products used (e.g. as coating). There were also several events where it was determined that tolerances were used that were not suitable, e.g. the tolerances were too small.

There were also four events where deflagration caused by H_2 build-up led to either inadvertent opening or to changes in the dimension of the affected valve(s).

Deficiency in construction or manufacturing of hardware (C/M)

A total of 11 events were identified as C/M. Eight of these were identified as a8, loose or degraded parts. Out of the eight events, there is one complete CCF event and one partial CCF event. The complete CCF resulted from improper hardening treatment during manufacturing, which lead to galling and the subsequent failure of the valve to stroke. The partial CCF resulted from rupture of the diaphragm on the actuator. The rest of the events also consisted of various manufacturing effects but it was not possible to establish any further findings, although two more events were linked to manufacturing defects of the diaphragm.

Deficient design modifications (D-MOD)

There are only two events identified as D-MOD. Both are complete impairments; however, one was caused by loose bolts (a8) and the other event by actuator equipment failure (a7).

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

	Failure mechanism category		
Failure cause categories	Movement of valve/pilot valve impeded	Valve/pilot valve leaking	Others
Deficiencies in design	**88**	**18**	**7**
D	Many events were identified as a8 (24/75). There are ten complete CCFs and 15 partial CCFs. 17 of the 24 events are linked to problems with diaphragms, including two of the complete CCFs. (75)	There is only one sub-category for this failure mechanism (13/13, b1). Low severity for all events. Six events are repeating events, which possibly shows deficiencies in safety culture. (18)	Problems relate to inadequate testing procedures or testing conditions. No failure mechanism (c2), in one case because there was no failure (only incipient). (7)
C/M	The majority of events (8/11) resulted from manufacturing defects resulting in loose or degraded piece parts (a8). Once complete and one partial CCF. Diaphragms was observed as a commonly affected part (3/11). (11)	-	-
D-MOD	One event resulting from loose bolts (a7) and one from actuator equipment failure (a8) following modifications. (2)	-	-

4.5. Failure analysis assessment of complete and partial CCF events

Understanding the complete CCFs is important for understanding plant risk as these events represent the most severe type of CCF events, where all components in a CCF group have failed. Examples of complete CCF events for SRVs include:

- Hydraulic testing (a non-routine job, although similar to testing during an annual outage) of steam SRVs involved installing a test gag but these were not removed after completion of the test, leading to the complete failure of a large number of SRVs.
- Following tests of SRVs it was found that they were set incorrectly. During the previous outage the wrong valve seat area had been used in the calculations for setting the valve for all valves. This same method was used at another reactor of the same type, making this a multi-unit event.
- All SRVs failed to open when tested. Investigation determined that the opening force from the valve actuator was too small, which was the result of an inadequate design of the actuator. Because all SRVs shared the same design, it was considered a complete CCF.

Table 4.6 shows the CCF root causes for the two highest severity event categories: complete CCF and partial CCF. There are no complete CCFs resulting from environmental triggers. The proportion of complete and partial CCFs is roughly equal for procedures and design triggers but higher for human actions, although the number of events is limited.

Table 4.6. Distribution of CCF root causes for complete and partial CCF events

CCF root cause		Complete CCF	Partial CCF
Design		**9**	**17**
DDD	Solely design	4	10
DDE	Predominant design and environment	0	3
DDP	Predominant design and procedures	4	1
DDU	Predominant design and unknown	1	3
Environment		**0**	**2**
EEP	Environmental trigger with procedure correction	0	1
EEU	Environmental trigger with unknown correction	0	1
Human actions		**4**	**5**
HHH	Solely human actions	2	1
HHP	Predominant human actions and procedures	2	4
Procedures		**4**	**7**
PPD	Predominant procedures and design	0	2
PPE	Predominant procedures and environment	0	0
PPH	Predominant procedures and human actions	1	1
PPP	Solely procedures	3	4
PPU	Predominant procedures and unknown	0	0
XXX	**No predominant CCF root cause**	**3**	**11**
Total		**20**	**42**

Table 4.7 shows the distribution events by failure mechanism category and failure cause category for complete and partial CCF events. When compared to Table 4.1 it is noticeable that the severity of events due to deficiencies in design, construction manufacturing (30 out of 113) is higher than for deficiencies in operation (26 out of 141). The severity of failure mechanism sub-categories O3 and D is also significantly higher than for other sub-categories. For O3 the share of high severity events is 45% (14 out of 31) and for D the share is 28% of events (28 out of 100).

Table 4.7. Failure analysis assessment matrix for complete and partial CCF events

	Failure mechanism category			
Failure cause categories	FM1 Movement of valve/pilot valve impeded	FM2 Valve/pilot valve leaking	FM3 Others	Total
Deficiencies in operation	**22**	**0**	**4**	**26**
O1	9	0	1	10
O2	2	0	0	2
O3	11	0	3	14
Deficiencies in design, construction, manufacturing	**27**	**2**	**1**	**30**
D	25	2	1	28
C/M	2	0	0	2
D-MOD	0	0	0	0
Unknown	**2**	**0**	**4**	**6**
Total	**51**	**2**	**9**	**62**

There are some larger groups of events with a common failure mechanism sub-category and failure cause category. For some groups of events it was possible to identify common aspects or weaknesses that may have played a significant role. Table 4.8 lists common findings from the failure analysis for complete and partial CCF events.

Table 4.8. Failure analysis assessment matrix, findings for complete and partial CCF event

Failure cause categories	Failure mechanism category		
	Movement of valve/pilot valve impeded	Valve/pilot valve leaking	Others
Deficiencies in operation	**22**	**0**	**4**
O1	• Failure to open due to rust/corrosion build-up around solenoid plungers. • Failure to open due to gumming up of lubricant in bearings • Failure to open due to adhesion/bonding between surfaces. (9)	–	• Testing was performed at an excessively high pressure, causing failure of the EPV to open. (1)
O2	• Continual exposure to high temperatures lead to increased degradation through heat stress of coil clearing contacts and diaphragm. (2)	–	–
O3	• Seven events relate to misalignment of components, a5. Of these, three events were caused by erroneous operator actions resulting in isolated valves. • Installation of the wrong part. • Improper connection or otherwise faulty maintenance. • Maintenance on the wrong valves. • Soluble paper used in connection with welding work was left, resulting in blocked steam drain pipes. (11)	–	• Test gags were not removed after tests were completed. • Two events resulted from SRVs made unavailable from operator actions due to testing outside of permitted test conditions. (3)

Table 4.8. Failure analysis assessment matrix, findings for complete and partial CCF event (Continued)

Deficiencies in design		**27**	**2**	**1**
	D	• Almost half of the events, eleven events, are related to I&C, a7, although the exact mechanism for the I&C failures are diverse. Examples include problems with faulty fuses and electronic cards as well as weak opening forces, e.g. resulting from bad solenoids. • Five events related to FM a8, with four due to degraded diaphragms. • Six events, both a4 and a1, were due to bonding and tolerance problems, primarily corrosion-induced. (25)	• Leakage from diaphragm and solenoid valve. • Blocked air cooling caused spring relaxation and opening of the valve, resulting in leakage. (2)	• Unknown cause but described as likely electrical interference/disturbance. (1)
	C/M	• Improper heat treatment. • Ruptured diaphragm. (2)	–	–
	D-MOD	–	–	–
Unknown		**2**	**0**	**4**

5. Summary and conclusions

CCF data have been collected for safety and relief valves, with organisations from Canada, Finland, France, Germany, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States contributing. In all, 271 ICDE events were reported from nuclear power plants (pressurised water reactors, boiling water reactors, Magnox and advanced gas reactors) and the data span a period from 1977 through 2015. The data are not necessarily complete for each country throughout this period. Compared with the data covered by the previously published SRV report (NEA, 2002), 122 new events are covered in this report.

The most common type of failure mechanism among all observed SRV events is FM1, movement of valve/pilot valve impeded (78% of events). The failure mechanism of the remaining events is roughly equally split between FM2, valve/pilot valve leaking, (12% of events) and others (10% of events). Within FM1, the three most common failure mechanism sub-categories are wrong set point of limit switch, torque switch maladjustment (21% of events); loose/broken/degraded screws, bolts, hinges, bushings, pistons, diaphragms, springs (19% of events) and I&C or actuator equipment failure (15% of events).

Although the share of events due to deficiencies in operations is slightly higher than due to deficiencies in design, construction and manufacturing, the latter has a slightly higher share for the more severe events. There, the causes for the more severe events are predominantly linked to diaphragms and I&C components. The diaphragms seem to suffer from ageing (due to temperatures), which could mean that updated and shortened maintenance intervals or changes to the design and material are likely to help mitigate such issues.

For the deficiencies in operations, the complete CCF events show strong indications of deficiencies in safety culture and training. For example, there were multiple events where maintenance activities were carried out on the wrong valves, valves were disabled (or in manual mode), tests were carried out under the wrong plant conditions and equipment installed for test purposes was not removed after completion of the test.

References

NEA (forthcoming), "Failure analysis coding guideline rev 8" (to be included in next revision of *ICDE General Coding Guidelines* as Annex 1).

NEA (2020), "Summary Record of the 68th Meeting of the Committee on the Safety of Nuclear Installations", NEA/SEN/SIN(2020)3, OECD, Paris (not publicly available).

NEA (2011), "International Common-Cause Failure Data Exchange ICDE General Coding Guidelines – Updated Version", OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_19122.

NEA (2002), "Collection and Analysis of Common-Cause Failure of Safety Valves and Relief Valves", OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_17748.

Annex A – Overview of the ICDE project

Annex A contains information regarding the ICDE project.

Background

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

To overcome these obstacles, the preparation for the international common-cause data exchange (ICDE) project was initiated in August of 1994. Since April 1998 the NEA has formally operated the project, following which the project was successfully operated over eight consecutive terms from 1998 to 2022. The current phase started in 2023 and is due to run until end of 2026. Member countries under the current Agreement of the NEA and the organisations representing them in the project are: Canada (CNSC), Czechia (UJV), Finland (STUK), France (IRSN), Germany (GRS), Japan (NRA), Sweden (SSM), Switzerland (ENSI) and the United States (NRC).

More information about the ICDE project can be found at the NEA website: www.oecd-nea.org/jcms/pl_25090/international-common-cause-failure-data-exchange-icde-project. Additional information can also be found at the website: https://projectportal.afconsult.com/ProjectPortal/icde.

Scope of the ICDE project

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

Data collection status

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

ICDE coding format and coding guidelines

Data collection guidelines have been developed during the project and are continually revised. They describe the methods and documentation requirements necessary for the development of the ICDE databases and reports. The format for data collection is described in the general coding guidelines and in the component specific guidelines. Component specific guidelines are developed for all analysed component types as the ICDE plans evolve (NEA, 2011).

Protection of proprietary rights

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

Annex B – Definition of common-cause events

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

- Unavailability of a specific set of components of the system, due to a common dependency, for example on a support function. If such dependencies are known, they can be explicitly modelled in a PSA.
- Unavailability of a specific set of components of the system due to shared causes that are not explicitly represented in the system logic model. Such events are also called "residual" CCFs. They are incorporated in PSA analyses by parametric models.

There is no rigid borderline between the two types of CCF events. There are examples in the PSA literature of CCF events that are explicitly modelled in one PSA and are treated as residual CCF events in other PSAs (for example, CCF of auxiliary feed water pumps due to steam binding, resulting from leaking check valves).

Several definitions of CCF events can be found in the literature, for example in NUREG/CR-6268, Revision 1 *Common-Cause Failure Data Collection and Analysis System: Event Data Collection, Classification, and Coding*: "Common-cause failure event: a dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause."

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

In the context of the data collection part of the ICDE project, focus will be on CCF events with total as well as partial component failures that exist over a relevant time interval[2]. To aid in this effort the following attributes are chosen for the component fault states, also called impairments or degradations:

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

Complete CCF events are of particular interest. A "complete CCF event" is defined as a dependent failure of all components of an exposed population where the fault state of each of its components is "complete failure to perform its function" and where these fault states exist simultaneously and are the direct result of a shared cause. Thus, in the ICDE project,

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

the aim is to collect complete CCF events as well as partial CCF events. The ICDE data analysts may add interesting events that fall outside the CCF event definition but are examples of recurrent – eventually non-random – failures. With growing understanding of CCF events, the relative share of events that can only be modelled as "residual" CCF events is expected to decrease.

Annex C – Failure analysis matrix – Deficiencies in operation

Failure cause	FM sub-category / Severity	Failure mechanism description	CCF Event Id	Total
SRV-a1	Deposits of dirt or oxidation products			4
	Partial CCF	Rust/corrosion build-up around the solenoid plungers due to the vendor failing to follow manufacturing procedures.	15008	1
		Soluble paper was used as a barrier in connection to welding work. When starting up, the paper blocked the drainage of the steam pipe, which then filled with water.	15044	1
	Complete Impairment	Valve did not close due to debris casing self-alignment to fail.	15025	1
	Incipient Impairment	Poor maintenance with insufficient heat insulation of some vital piping and components adjacent to the valve caused condensate water in the upper part of the main valve.	15127	1
SRV-a2	Missing or degraded lubrication			7
	Partial CCF	Gumming-up of the lubricant at the bearings (sluggishness of its upper radial bearings and the rolls of the lower radial bearing stuck).	16088	1
	CCF Impaired	An unsuitable grease (not qualified for use in required temperatures) for greasing the O-ring seal led to sticking of the valves.	15033	1
		High temperature caused gumming-up of the lubricant and, consequently, jamming of the valve.	16103	1
		Inappropriate grease by the manufacturer caused volatile ingredients to vapourise, leaving a highly viscous film, which led to gluing of the solenoids and anchors of the contactors.	16334	1
		O-ring fragments in the grease of the axial bearing and O-ring stripping of the spindle caused friction, which led to tripping of the torque-limitation-switch.	15050	1
	Complete Impairment	Degradation of anti-seize compound, resulting in an increase in friction between the sliding surfaces, and hence an alteration in the valve characteristic which caused valve setting to drift.	15111	1
		Hardened grease in the valves' axial bearings led to increased running torque.	16248	1
SRV-a3	Scratched or degraded seat/disk/O-ring/seal surfaces			5
	Complete Impairment	Combination of poor design, installation and testing procedure led to residue and thermal expansion of valve discs.	16294	1
		Cracking of the main disks.	15010	1
	Incipient Impairment	Air leakage from the valve positioners due to loose fittings and worn seals.	15063	1
		Old brittle O-rings in the valve actuator allowed air to leak out, degrading operation (valves drifted shut).	15006	1
			15037	1
SRV-a4	Bonding			3

Failure cause	FM sub-category / Severity	Failure mechanism description	CCF Event Id	Total
	Partial CCF	Adhesion between spindle and nut caused the bonding between the valve seat and valve disk to increase, resulting in triggering the torque switch.	15939	1
	CCF Impaired	The cone was stuck in its guide.	15053	1
	Incipient Impairment	Too tight packing, from previous maintenance, led to binding of the valve stem and stem collar.	15143	1
SRV-a5	Misalignment of switches, disk or in valve settings			19
	Complete CCF	Main disc guide (piece-part of PORV) installed incorrectly on both valves during maintenance activity (neither valve could be opened).	15013	1
		Mispositioning of control air led to isolated valves.	16362	1
		The auto-manual control station of the emergency panel had been left in manual position after a test which led to a no synchronism between two buses of the control block rack panel.	15005	1
		Valves were unavailable at the same time by human error (maintenance operations were carried out by mistake on the wrong valves).	15085	1
	Partial CCF	A maladjustment of the switching at the transformer caused a short-circuit resulting in in-operable valves.	15122	1
		Improper connection of nitrogen lines to the two valves due to human error.	15066	1
		In one of the four main steam safety valves stations all pilot lines were erroneously isolated by the respective hand valves.	15125	1
		No underlying reason could be found.	15128	1
	Complete Impairment	Instrument air leak prevented the SRV from holding open (EWS requirements not met).	15030	1
			15036	1
			15146	1
		Insufficient quality control during valve refurbishment and incorrect re-assembly following maintenance caused inadequate valve travel length, resulting in insufficient discharge capacity.	15001	1
			15028	1
			15161	1
			15164	1
		Over-torqueing of the warped diaphragm chamber base of the valve led to a bent valve stem resulting in a valve seating mismatch.	15027	1
		Pressure switches of pressure relief valves remained in isolated state after installation.	15388	1
		Valves had strokes outside the design tolerances resulting in reduced discharge capacity.	15108	1
	Incipient Impairment	Misalignment of valves by contractor.	15991	1
SRV-a6	Wrong set point of limit switch, torque switch maladjustment			50
	Complete CCF	An incorrect valve seat area was used in the calculations required for setting the valve.	15385	1
			15386	1
		The main steam pressure the relief valves failed to close due to tripping of the valve motor by the torque-limitation-switch (torque value was adjusted too low).	15126	1
	CCF Impaired	Valve lift settings set incorrectly (un-lagged instead of lagged) by manufacturer which led to too low lift.	15078	1

Failure cause	FM sub-category / Severity	Failure mechanism description	CCF Event Id	Total
	Complete Impairment	Inappropriate setting leading to a non-concurrence to the requirement.	15112	1
		A wrong scaling factor in the equipment for testing the set points of steam generator safety valves led to setting of excessively low set points of the valves. This was only detected when the testing equipment was replaced by a new one with a new testing method.	15120	1
		An audit revealed cases where combination of valve settings did not comply with operating rule.	15047	1
		Calculation error due to inaccuracy in mean seat area constant caused all valves to be 1-3% out of tolerance.	15135	1
		Confusion between pressure units (bar and psig) led to the SRV's settings not to comply with operating rule.	15114	1
			15116	1
		Inadequate original procedures to calibrate and test a built-in fail safety feature was found out to potentially actuate the valves spuriously at a low set point during certain conditions.	16398	1
		Maintenance instructions not updated, leading to a wrong setting of 2 SRV's opening pressure (other problem: accuracy of the test method may be not sufficient).	15077	1
		New procedure was used that led to slightly higher lift set points. However, the licensee indicated set point drift could not be ruled out.	15167	1
		Opening pressure for the safety valves was set too high due to inadequate testing method.	15073	1
		Pilot valve settings drifted out of tolerance.	15381	1
		Reduced discharge capacity due to wrong measurement of valve lift.	15068	1
			15090	1
			15107	1
			15151	1
		Safety valves did not lift when the indicated steam pressures were in excess of the normal set lift pressures due to setting procedure error.	15389	1
		The actuator had an incorrect setting of the opening torque switching due to human error.	16323	1
		The safety valve 'set pressure' was set too low.	15113	1
		The valves lift was above the set pressure.	15380	1
		Valves drifted outside operating rule limit.	15110	1
			15165	1
		Valves exceeding set point values.	15390	1
		Valves opened before set values.	15179	1
	Incipient Impairment	Drift of the set point due to a wrong calibration bench.	15089	1
		Inadequate procedure to calibrate the safety valves (applied in different conditions of testing without the precision needed).	15048	1
		Main steam safety valves failed surveillance testing due to high lift pressure caused by faulty information supplied by vendor.	15129	1
		Main Steam Safety Valves were set incorrectly due to poor training and bad procedure.	15096	1
		Opening pressure outside the permitted range (cause unknown).	15144	1
		Safety valves were outside of permitted set point values.	15076	1

Failure cause	FM sub-category / Severity	Failure mechanism description	CCF Event Id	Total
		Set point of valve lift (cause unknown).	15069	1
		Set point settings of pressure found over the limit of allowed operating conditions due to drift.	15018	1
			15021	1
			15029	1
			15106	1
			15133	1
			15149	1
			15166	1
		Set pressure value was over the limit of operating conditions.	15152	1
		Valve lift settings set incorrectly (un-lagged instead of lagged) by manufacturer, which led to excessively low lift.	15091	1
		Valves exceeding set point values.	15119	1
			15142	1
			15153	1
			15170	1
		Valves exceeding set point values. Experience shows the valves work "easier" after they had been exercised. Some jam in valve stem/valve stem bush can occur.	15141	1
		Valves opened before set values.	15178	1
		Wrong set point setting (over set pressure value of operating conditions) due to incomplete procedure and wrong use of calibration bench.	15100	1
SRV-a7	Logic (I/C) and control (actuator) equipment failure			18
	Complete CCF	Continual energisation to the relays coil clearing contact, which degraded as a result of continual high temperatures over time, led a relay in the Steam Dump Control Panel to fail.	16364	1
		Surge suppression diodes installed on the electric Lift actuation relays failed.	16385	1
	Partial CCF	An incorrect lower adjustment ring setting, caused by inadequate work control by the vendor, led to a faulty power supply in the Electro-Hydraulic Control (EHC) system resulting in closure of the turbine valve.	15079	1
		Maintenance personnel installed wrong piece-part in both valves, resulting in failure to open.	15022	1
		Valves in the system were put in position to forced closure of the main valves. Due to leakage in control valve, the main valves inadvertently opened.	15156	1
	CCF Impaired	Safety relief valve actuators could not be latched open (cause unknown).	15130	1
		Ageing of the modutronic (piece-part of the controller) caused loss of auto-control function.	15136	1
		Ageing problem of the anchor sealing caused slow operation of magnet valves.	15088	1
	Complete Impairment	A maintenance staff error where a tool was dropped on a temporary protective plate below (in spite of the protection), caused a circuit breaker to disconnect the magnetic loads.	16395	1
		Ageing problem of the anchor sealing caused slow operation of magnet valves.	15147	1

Failure cause	FM sub-category / Severity	Failure mechanism description	CCF Event Id	Total
			15154	1
			15162	1
		Excessive pneumatic actuator accumulator leakage due to normal wear and ageing resulted in possible failure to open PORV.	15462	1
		Main Feed water Pump (MFP) speed control mechanism failed, causing erratic steam dump operation, which resulted in low-low steam generator level trip.	15057	1
		Malfunction of the positioners resulted in an external leakage.	15014	1
	Incipient Impairment	Human error concerning the Pressuriser Master Controller.	15064	1
		PORVs did not provide the minimum required steam flow capacity to support the DBA analysis.	15083	1
		The sensor was mounted on each safety valve with a displacement (non-respect of the required air-gap) leading it to be out of operating conditions.	15132	1
SRV-a8	Loose/broken/degraded screws, bolts, hinges, bushings, pistons, diaphragms, springs			18
	Complete CCF	Incorrect installation of the modified diaphragm led to failure of fully open the valves.	15031	1
		Incorrect torqueing of actuator flange (actuator diaphragm bolts were loose) which allowed air leakage resulting in PORVs to fail to open.	15163	1
	Partial CCF	Inadequate procedure and design caused diaphragm on the actuator to rupture.	15461	1
		Wear (due to age) and abnormal heat stress led to leaking actuator diaphragm.	15060	1
	CCF Impaired	Insufficient crimping of the locknut led to the pilot valve and the main valve to come apart.	15040	1
		Loose hold down nut led to failure to reclose.	15015	1
		Piston ring had loosened and broken into pieces, which led to a loose part falling down to the main cylinder and jamming the piston to the cylinder wall.	15038	1
		Valve failed to open due to loss of hydraulic fluid when tubing failed from vibration and wear.	15070	1
	Complete Impairment	A non-straight spring caused increased friction, which led to valve stem lying hard against the upper bushing (scratch marks).	16431	1
		Air leakage from actuator diaphragm.	15464	1
		An incorrect link bushing gap led to instrument air accumulator check valves to be incapable of isolating the accumulators.	16367	1
		CO_2-leak due to missing a pop test tapping point plug.	15384	1
		Valve opened too early (the spring may have been affected by heat and static load which may have been temporary, but could also be a beginning of a continuous relaxation).	16432	1
		Wear on posts, bushings and plunger of the actuators.	16360	1
	Incipient Impairment	Air leaks due to loose diaphragm bolts.	15985	1
		Normal wear and ageing of diaphragm and O-ring seal.	15059	1
		Part change caused increased friction force and thus piston required more moving force.	15145	1
		Worn internal parts due to normal wear led to valves exceeded the required stroke time.	15016	1
SRV-b1	Valve leaking due to seat/disk/O-ring/seal surface degradation			15
	CCF Impaired	Both valves were leaking air past O-rings in the positioners.	15023	1

Failure cause	FM sub-category / Severity	Failure mechanism description	CCF Event Id	Total
	Complete Impairment	Ageing of the O-ring led to it to become brittle, resulting in air leaks.	15158	1
		Directly after the service, the opening pressure is adjusted, causing the valve spring to not have enough time to stabilise itself after the compression, resulting in a small leakage.	16429	1
			16430	1
		Internal leakage in closed position (cause unknown).	16327	1
		Marks on the sealing surfaces of the valve led to small leakage.	16428	1
		Significant leakage past the valves due to seat cutting of the seats.	15459	1
		Wear at the valve cone caused a very small leakage, which led to decrease of opening pressure.	15087	1
			15121	1
	Incipient Impairment	Excessive seat leakage due to improper assembly.	15458	1
		Manufacturing related residual stress in the pipes in combination with a concentration of fluorine due to an earlier used fluorine lubricant caused the cracks in the pipes resulting in a leak.	15062	1
		Operation too close to set point and valve end loading/stress resulted in leakage.	15134	1
		Unadjusted emergency relief valves (due to deficient maintenance) and a failed vacuum breaker (due to failed internal spring) resulted in leakage.	15074	1
		Wear at the valve cone caused a very small leakage, which led to a decrease of the opening pressure.	15012	1
			15055	1
SRV-c2	Other/unknown			19
	Complete CCF	A pressure test was carried out that involved gagging steam SRVs, but these were not removed.	15115	1
		Human error due to test under wrong plant conditions (operators did not check the initial conditions for performing the test).	15061	1
		Main Steam Safety Valves not reseating (cause unknown).	16369	1
	Partial CCF	No opening of the main valves was obtained during test (cause unknown).	16322	1
		Operator error resulted in no SRVs being available on two steam generators.	15093	1
		Test was performed at a slightly too high pressure, which caused the electromagnetic pilot valve not to open.	15104	1
		Testing of pilot valves with reduced voltage led to valves not opening (no specific cause detected).	16329	1
		Three of four liquid relief valves (LRVs) failed to stroke during monthly heat transport LRV stroke test (cause unknown).	15067	1
	CCF Impaired	High temperature due to the drip pan covers resulted in malfunctioning electromagnetic pilot valve.	15035	1
		The safety valve was inadvertently removed due to workers doing work on the wrong component, resulting in water cascading down.	15168	1
	Complete Impairment	An attempt to re-seat two leaking relief valves in the RCS failed.	15045	1
		Inadequate testing procedure (no opening time was specified).	15071	1
		No direct cause can be established to explain lifting of the valves.	15109	1
	Incipient Impairment	Air hold test failed due to the valves did not remain open wide enough to allow installation of latches (cause unknown).	15905	1

Failure cause	FM sub-category / Severity	Failure mechanism description	CCF Event Id	Total
		Air receivers failed to keep the relief valves open (cause unknown).	15901	1
			15902	1
		During safety system testing of the SRV actuators, the valve could not be latched open (some leaks were found in the system but nothing too definitive).	16000	1
		Safety relief valve was found passing (cause unknown).	15998	1
		There is no real failure mechanism as this was the result of a wrong procedure used to determine the set points of the SRVs.	15020	1
Grand Total				158

Annex D – Failure analysis matrix – Deficiencies in design, construction and manufacturing

Failure cause	FM sub-category/ Severity	Failure mechanism description	CCF Event Id	Total
SRV-a1	Deposits of dirt or oxidation products			13
	Partial CCF	Corrosion in the magnetic anchor, which caused tight tolerances of the magnetic anchor.	15007	1
			15034	1
			15049	1
	CCF Impaired	A pilot valve failed to open due to adhesive coating on valve actuator.	15848	1
		Corrosion and significant moisture within the operating mechanisms.	15383	1
		The spiral spring of the valve is preserved with coating of zinc powder, which oxidized under reactor operation temperature.	15148	1
	Complete Impairment	Corrosion due to vibrations, which led to hammering of the magnet plunger and thereby to an abrasion of the guide bushing. The abraded material built a coating on the magnet plunger, which delayed the movement of the armature.	15849	1
		Crystalline deposit on the valve disk and seat, which is believed to have caused the low lift pressure.	15382	1
		Debris build-up in the system caused the valves to not re-seat correctly	15387	1
		The material combination used for armature bar and bushing was susceptible to vibrations which led to corrosion (fretting/pitting).	15131	1
	Incipient Impairment	Foreign material in seating area due to expected wear.	15043	1
		Foreign material intrusion, corrosion, seat/disc alignment and vibration caused seat leakage leading to elevated temperatures, spring relaxation and set point drift.	15101	1
		Manufacturing process leading to corrosion	15940	1
SRV-a3	Scratched or degraded seat/disk/O-ring/seal surfaces			2
	Complete Impairment	Problems in pilot valve seats caused set point drift	16388	1
			16413	1
SRV-a4	Bonding			12
	Complete CCF	Seat bonding, which was characterised by the formation of an oxide adhesion layer between metal parts.	16379	1
	Partial CCF	Corrosion-induced bonding of the surface between the pilot valve disc and seat led to SRV set point drift.	15054	1
		Metallurgical bonding between the MSSV disc and seat (believed cause) led to valves not lifting when adequate force was applied.	15159	1
		Some tolerance limits (cylinder, bearing) were not optimal.	15123	1

Failure cause	FM sub-category/ Severity	Failure mechanism description	CCF Event Id	Total
	CCF Impaired	Corrosion-induced bonding.	15004	1
	Incipient Impairment	A sticking phenomenon between the main steam safety valve (MSSV) nozzle and disc seats caused high initial lifts.	15124	1
		Corrosion bonding at disc/seat interface.	15011	1
		Corrosion-induced bonding (disc-to-seat oxide) led to SRVs set points to drift.	15002	1
			15009	1
		Corrosion-induced bonding of the surface between the pilot valve disc and seat led to SRV set point drift.	15046	1
		Metallurgical bonding between the MSSV seat and the disc led to set point drift.	15080	1
		Seat bonding led to drifted set points.	15094	1
SRV-a6	Wrong set point of limit switch, torque switch misadjustment			6
	Partial CCF	Normal use and cyclic fatigue led to set point drift.	15099	1
		Normal wear led to safety valve to be out of lift set points.	15058	1
	Complete Impairment	All SRVs were found out of tolerance of the set points due to drift.	15172	1
		Adjustment of torque setting values to the maximum value of the actuator caused relaxed springs, which led to actuators to be outside the limit of maximum deviation.	16321	1
	Incipient Impairment	MSSVs setpoint drift.	15084	1
		The valve lift set point drifted low.	15896	1
SRV-a7	Logic (I/C) and control (actuator) equipment failure			22
	Complete CCF	Bad solenoid (piece-part) on the valve actuator, possibly due to ageing, led to PORVs' failure to close.	15075	1
		Block switch failed, which prevented PORVs from automatic actuation to prevent low temperature over pressurisation during shutdown.	15463	1
		Blown fuse resulted in valves' failure to open.	16397	1
		Error in design of the switch contact in the control block rack, resulting in failure to open.	15082	1
		Faulty fuse of the control system rack led to inoperability of the valves.	15171	1
		The opening force from the valve actuator was too small and the pilot plug holes and the main plug holes, through which the fluid passes from the pressurised cavity to the low pressure side of the valve, were not adequate to relieve the valve cavity pressure	15157	1
	Partial CCF	Detached booster relays which had been subject to low ambient temperatures during a period of little use resulted in failure to open.	15095	1
		Relay fault (possibly due to ageing) caused inadvertent opening of valves.	15098	1
		The electronic card in the control-instrumentation failed to actuate the quick pulses and the valves maintained in open position.	15072	1

Failure cause	FM sub-category/ Severity	Failure mechanism description	CCF Event Id	Total
		The opening force from the valve actuator was too small and the pilot plug holes and the main plug holes, through which the fluid passes from the pressurised cavity to the low pressure side of the valve, were not adequate to relieve the valve cavity pressure.	15052	1
			15081	1
	CCF Impaired	Drifting of the micro switch settings and an improper contact led to inoperability of relief valves.	15118	1
		Excessive main steam line vibration resulted in damage and potential inoperability of all four electromatic relief valve actuators at both units.	16375	1
			16376	1
		The I/P-converter was clogged due to deposition/coating.	16427	1
		Vibrations of the solenoid probably caused adhesive coatings (organic and metallic constituents) and abrasion of the guide bushing which resulted in blocked movement of the armature of the solenoid actuator of the pilot valve.	15847	1
	Complete Impairment	Incomplete design not taking into account all possible accident conditions reduced the capacity of the safety function leading into incomplete opening of the safety valves.	15937	1
		Leaks in back-up air tanks could not be detected due to inadequate installation combined with inadequate commissioning testing resulting in failure to open the valves.	15041	1
		The valve stem revolved, which caused the feedback lever to turn and the valve positioner out of its position, which meant that the valve could not be controlled remotely.	16433	1
		The vendor installed valve stems whose length was one inch short of allowing full stroke of the valves.	15039	1
	Incipient Impairment	An intermittent failure in the control cubicle could have caused the spurious activation.	15019	1
		Internal part of the valve was malfunctioning which led to air leaks from the actuator.	15895	1
SRV-a8	Loose/broken/degraded screws, bolts, hinges, bushings, pistons, diaphragms, springs			33
	Complete CCF	Air leakage around valve operator due to loose bolts.	15051	1
		Flaw in the diaphragm sealing area.	15169	1
		Improper heat treatment during the manufacturing of new valve guide bushings resulted in low hardness, which then produced galling and subsequent failure of the valves to stroke	15032	1
		Stretched bolt holes were seen in all failed diaphragms caused by loose bolts due to high compression set of the EPDM material used in the valves which led to air leakage.	15056	1
	Partial CCF	Heat damage/degradation led to dry and cracked diaphragm of the regulator.	15139	1
		Rupture of the diaphragm on the actuator.	15092	1
		Ruptured diaphragm.	15140	1
	CCF Impaired	A faulty diaphragm in the actuator of relief valve led to an actuator air leak causing the relief valve to close.	15150	1
		Manufacturing defect in the diaphragm.	15137	1
		Rupture of the diaphragm on the valve operator due to wear	15138	1

Failure cause	FM sub-category/ Severity	Failure mechanism description	CCF Event Id	Total
		The electromagnet of the pilot valve was stuck due to an exceedingly small clearance between socket and shaft caused by the fact that the electromagnets were run by a closed-circuit principle and so continuously exposed to additional heat, which led to an expansion.	16087	1
	Complete Impairment	After a modification the SRV was not able to stay in an open position as required as the modification caused bolts to extend from the bottom of a flange more than before.	15910	1
		All valves had loose diaphragm bolts and a faulty diaphragm.	15912	1
		Excessive leakage of the instrument air check valves due to inadequate actuator diaphragms.	16004	1
		Leaking or faulty diaphragm	15904	1
		The diaphragms of the valves were deteriorated due to the aluminum cap was replaced with a stainless steel cap leading to higher temperatures than normal.	16389	1
			16414	1
	Incipient Impairment	One valve had a passing check valve and loose actuator cover bolts and the other valve had diaphragm leaks around the valve actuator cover bolts.	15900	1
		A leaking or faulty diaphragm.	15906	1
		All valves had air leakage in the valve diaphragm caused by loose diaphragm bolts.	15911	1
		All valves had loose inner and outer diaphragm bolts.	15907	1
		Cracks in the stellite facing of the globe valve disk bushing of main steam relief valve.	15065	1
			15103	1
		Four of the six valves had loose diaphragm bolts and the other two valves a passing check valve.	15899	1
		Hydrogen induced stress-corrosion cracking led to broken closure spring and its spring force was reduced.	16475	1
		Leaking diaphragm.	15897	1
		Leaking or faulty diaphragm.	15913	1
		Loose bolts and the cam being slightly out of adjustment.	15908	1
		Normal wear led to gradual deformation of the air diaphragm.	15042	1
		Two of the three valves had loose diaphragm bolts and the third valve had loose diaphragm bolts and a leaking solenoid valve.	15898	1
		Two of the valves had loose diaphragm bolts and on the other valve the diaphragm was degraded.	15909	1
		Two of the valves had loose diaphragm bolts and the third valve had elongation of the diaphragm bolt holes.	15903	1
		Vertical scratches at the piston rings and wear at the guide bushings of the cylinder cone and of the piston led to delayed opening times.	15003	1
SRV-b1	Valve leaking due to seat/disk/O-ring/seal surface degradation			18
	Complete CCF	Leakage from each of the SRV's actuator diaphragm and solenoid valve.	16352	1
	Partial CCF	Insulation around the impulse valve blocked the air cooling of the spring, causing relaxation and inadvertent opening of the valve and leakage.	16326	1

Failure cause	FM sub-category/ Severity	Failure mechanism description	CCF Event Id	Total
	CCF Impaired	Corrosion at the weld between ferritic and austenitic steel (between the pilot valve and the pilot pipe) led to a small leakage.	16099	1
		SRV seat leakage caused by a combination of insufficient simmer margin and lack of full insulation coverage.	16356	1
	Complete Impairment	Excessive leakage past the in-body gasket due to improper design.	15460	1
		External leakage in a connection at the steering pipe (and defects in insulation) caused condensation which led to extended opening times of the valves.	16330	1
		External leakage in either the valve or the connecting pipe system.	16328	1
		Increased condensate accumulation in the valve chamber led to extended opening times of the valves.	16331	1
		Slight obliquity between the valve seat and the valve head of the release section caused the valve spring to end up in a slightly incorrect position, which led to a small leakage.	16426	1
		Stresses induced in the valve by the discharge line (suspect external piping loads deformed valves) resulted in-body/seat flexing and leakage.	15086	1
	Incipient Impairment	Chloride induced stress-corrosion cracking led to leakage on control line of electromagnetic pilot valve to safety and relief valve.	16476	1
		Flow-assisted corrosion due to wrong material combination of valve cone and valve seat, resulting in seat leakage.	15160	1
		Leaking due to inadequate design of the pilot plug and pilot base.	15017	1
		Pilot seat erosion led to leakage.	15155	1
		Radial cracks in nozzle seating surfaces led to leakage.	15097	1
		The cause for long operating time was condensed water which had leaked through EPV to the inside of the main valve	15024	1
		The check valves had scoring on the seating surfaces from foreign objects.	15026	1
		Valves had cracking in nozzle which led to leakage.	15102	1
SRV-c1	H_2 build-up			4
	CCF Impaired	Deflagration occurred in the indication housing of the valve, causing inadvertent opening of the valve.	16333	1
	Complete Impairment	Small deflagration (rapid burning) caused dimension change (thin-walled material) in the electrical pilot valve.	16332	1
	Incipient Impairment	It is likely that hydrogen gas deflagration has occurred when condensate accumulated in the valve, causing it to become cooled so that the recombiner (some deformation of the platinum spiral) no longer worked.	16324	1
	Single Impairment			1
SRV-c2	Other/unknown			3
	Partial CCF	Valves unexpectedly opened while at power (cause unknown but likely cause could be electrical disturbances).	15105	1
	CCF Impaired	Cause for long operating time is unknown.	15117	1
	Complete Impairment	Test with reduced voltage revealed that one of the pilot valve's coil to have a lower resistance which suggests that the main valve may have been warmer than the rest leading to failure to open.	16325	1
Grand Total				113

Glossary

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

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

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

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

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

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

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

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

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

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

***Failure cause categories*:** A high level and generalised list of the deficiencies in operation and in design, construction and manufacturing that caused an ICDE event.

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

***Failure mechanism categories*:** Component type-specific groups of similar failure mechanism sub-categories.

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

Failure mode: The function the components failed to perform.

ICDE event: All events accepted into the ICDE database. This includes events meeting the typical definition of a CCF event (as described in Appendix B). ICDE events also include less severe events, such as those with impairment of two or more components (with respect to performing a specific function), that exist over a relevant time interval and are the direct result of a shared cause.

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

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

Root cause: The fundamental 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: Allows the analyst to express a degree of confidence about the multiple impairments resulting from the same cause.

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