Unclassified **NEA/CSNI/R(2004)4**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **30-Jan-2004**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2004)4
Unclassified

INTERNATIONAL COMMON-CAUSE FAILURE DATA EXCHANGE

ICDE GENERAL CODING GUIDELINES - TECHNICAL NOTE

JANUARY 2004

JT00157469

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14 December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of 28 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

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

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

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different Member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

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

* * * * * * * * * * * *

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux
France

ICDE GENERAL CODING GUIDELINES

FOREWORD

In this document, the general coding guidelines for the OECD ICDE-Project (International Common Cause Failure Data Exchange) are presented with explanations and appendices for each analysed component. The guide reflects the present experience with the already completed data collection.

The following persons have significantly contributed to the preparation of the main guidelines by their personal effort, for which they deserve an acknowledgement: Mr. Gunnar Johanson (ES Konsult), Dr. Wolfgang Werner (SAC), Mrs. Marina Concepcion Capote (ES Konsult / Emarcon) and Dr. Albert Kreuser (GRS).

In addition, those persons who have contributed to the component specific guidelines are mentioned in the respective appendices ICDECG 01-06 of this document. Finally, the ICDE Working Group and the people with whom they liaise in all participating countries are recognized as important contributors to the success of these guidelines.

TABLE OF CONTENT

1. INTRODUCTION

Several Member countries of the Nuclear Energy Agency of the Organisation for Economic Co-operation and Development ("OECD/NEA") have established the International Common-Cause Failure Data Exchange Project ("ICDE Project") to encourage multilateral co-operation in the collection and analysis of data relating to Common-Cause Failure (CCF) events.

The objectives of the ICDE Project are to:

a) Collect and analyse CCF events over the long term so as to better understand such events, their causes, and their prevention;
b) Generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences;
c) Establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defences against their occurrence, such as indicators for risk based inspections; and
d) Record event attributes to facilitate quantification of CCF frequencies when so decided by the Project Working Group.

The ICDE Project is envisaged to comprise all possible events of interest, including both complete and partial ICDE events. An "ICDE" event is defined in the next section.

The ICDE Project will cover the key components of the main safety systems. Presently, the components listed below are included in the ICDE Project. Data have been collected for the six first components in the list.

- Centrifugal pumps
- Diesel generators
- Motor operated valves
- Safety relief valves/power operated relief valves
- Check valves
- Batteries
- Level measurement
- Breakers
- Control rod drive assemblies

Others will be added to this list later on.

In this component coding guidelines, explanations on the ICDE General coding format are given. The guide reflects present experience with the data format and with the collected data. Further interpretations and clarifications will be added, should they become necessary.

For each component analysed in the ICDE project, separate coding guidance is provided in the appendices ICDECG 01-06, specifying details relevant to the respective components.

2. DEFINITION OF COMMON CAUSE EVENTS AND ICDE EVENTS

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

1. 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.

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

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

In the context of the data collection part of the ICDE project, complete as well as potential CCF events will be collected. To include all events of interest, an "ICDE event" is defined as follows:

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

1) Possible attributes of impairment are:

- *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*

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

The ICDE data analysts may add interesting events that fall outside the ICDE 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.

3. DEFINITION OF OBSERVED POPULATION (OP), COMMON CAUSE COMPONENT GROUP(S) (CCCG) AND EXPOSED POPULATION (EP)

The basic unit for collecting ICDE events is an Observed Population, a fixed number of similar or identical components within one system potentially exposed to the same failure mechanisms.

Sets of similar observed populations form the statistical basis for calculating common cause failure rates or probabilities. (For some calculating models not all the information about the components in the observed populations provided in the observed population records is necessary such as a time period indicating the observation time and independent failure counts.)

For each included ICDE component type a specific component coding guideline is developed, defining the OP to be used for ICDE event collection (CCCG or EP), the component boundaries, event boundary, coding rules and exemptions, functional fault modes.

For example, for the collection of pump and diesel generator data the Observed Population is defined using CCCGs. For the collection of MOV data the Observed Population is - due to practical reasons - defined by the Exposed Population (event by event).

Definitions

To allow for data collection needs and for CCF-quantification needs for all types of components, the following concept of "Population" is used with the definition as given below.

- **Observed Population**

The **Observed Population (OP)** is a set of similar or identical components. The OP is needed to provide the statistical basis for some of the models for quantification of CCF probabilities. Not every model requires all the information about the components provided in the observed population records.

In general, an OP is a collection of all similar components within one system (e.g. all MOV in the Auxiliary Feed Water System or all pumps in the Residual Heat Removal System), but there may be cases of OPs containing components of more than one system.

- **Exposed Population**

An **Exposed Population (EP)** is a set of similar or identical components actually having been exposed to the specific common causal mechanism in an actually observed CCF event. All components of an EP are exposed to the common causal mechanism, but may be affected differently: some may fail completely, some may become degraded, and others may remain unaffected. EPs are a data collection concept and are used for reporting events, their composition is defined by the reported event and is described by the component impairment vector (the length of which is equal to the size of the EP). The impairment attribute "working" is assigned to those components in the Exposed Population that were not actually affected by

the CCF event. The components of the EP may perform different functions, for example, an EP may contain suction and discharge valves. The following general compositions of EPs are encountered:

a) The EP is equal to the specific CCCG for which the event was reported.

b) The EP is the particular subset of components of an OP that were exposed to the common causal mechanism of the event.

A **Common Cause Component Group (CCCG)** is a set of components that are considered to have a high potential for failure due to a common cause (with several different common causes being possible). In most cases the components of CCCGs are redundant, identical components of a system, all performing the same function. Example: parallel pumps in a multi-train injection system. CCCGs are used for reporting events, as well as for defining OPs.

The rationale for introducing CCCGs is:

a) Groups of redundant, identical components of a system, all performing the same function, are explicitly modelled in many probabilistic safety analyses

b) By their very nature, all components of a CCCG are expected to be exposed to the same common causal mechanisms. (exceptions are possible).

c) In some cases, an OP, EP and CCCG are identical (e.g., pumps, EDGs).

d) When possible or appropriate the OP may be defined by Common Cause Component Groups.

4. OBSERVED POPULATION IDENTIFICATION RECORD OR CCCG IDENTIFICATION RECORD

The fields G0 - G7 are developed once. In exceptional cases it may be necessary to update the component description in field G1 to make the degree of detail consistent with the degree of detail in the description of an initially not envisaged event (field C5).

G0 Observed Population/CCCG identifier

Code/Automatic

Identifier with reference to country, plant, system and component.

G1 Observed Population/CCCG definition

Text/Compulsory

The Observed Population is a set of similar components in the same system in the same plant that performs the same function.

One or several Common Cause Component Group(s) (CCCG) defines the Observed Population, or, when this is not possible the Observed Population is defined by one record for each system and each type of component.

Specific reference to country, plant, system and component shall be given.

Component type, size of the Observed Population/CCCG, manufacturer and a detailed description of the components are to be provided, including the component boundary. The degree of detail of the description must be such that the event description(s) can be fully understood.

For the component boundaries it is recommended to use the definitions given in the Swedish T-Book (See references), but other boundaries are also acceptable, if clearly defined. See also the separate component coding guidelines.

The Observed Population/CCCG are the basic sets of components in the context of CCF data base set-up and analysis. The size of the Observed Population/CCCG is the number of similar/redundant components in the system that are potentially susceptible to the same failure mechanism. The Observed Population/CCCG is assumed to be internally homogenous. The Observed Population can contain components of different systems serving different functions.

If there is permanently aligned shared equipment at multi-unit plants, it shall be considered at unit 1, see field G2.

If the system has multiple functions (e.g. Residual Heat Removal and Low Pressure Safety Injection) this should be indicated.

G2 Plant(s)

Code/Compulsory

The plant code is the code of the nuclear power plant where the CCF event occurred. IAEA/NEA IRS coding, (e.g. NEA/CSNI/R(1997)12) is used.

G3 System type / function

Code (Vector)/Compulsory

The system field describes the group of components in the Observed Population, including the failed component, that work together to perform a specific function. There may be reference to national coding (in G1). A searchable sub-field contains the IRS code

G4 Component type

Code/Compulsory

The component field describes the equipment that experienced the CCF event. The code refers to system components that are normally modelled in probabilistic safety assessments.

The description may contain reference to national coding. A searchable sub-field contains the IRS code.

For each component evaluated in the ICDE project, e.g. pumps, EDG, MOV etc, a specific list of types is generated allowing to differentiate equipment according to important technical features e.g. centrifugal pumps, globe valves, gate valves and ball valves.

G5 Testing

G5-1 Test interval

Days/Compulsory

The test interval for the individual components in the Observed Population/CCCG should be given. It is the period between two consecutive tests of one component.

G5-2 Test procedure

Checkbox/Compulsory

The test procedure will have two alternatives:

1. Staggered or

2. Sequential (non staggered)

In the analysis part, this information - together with C2, date of event(s) - is typically used to measure the “degree of simultaneity” of CCF events.

If there is more than one mode of testing (Start test, Capacity test, etc.) the shortest test interval shall be given.

If a CCF failure phenomenon can only be detected in a "larger" test this is indicated by the C6-Detection coding as a part of the rationale to classify the event as common cause event.

G6 Size of Observed Population/CCCG

Numeric (Compulsory in G1)

The size of the Observed Population/CCCG is the number of similar/redundant components in the system. The Observed Population/CCCG is assumed to be internally homogenous. The size of the Observed Population/CCCG is the number of components in the systems of the plant that are potentially exposed to the same failure mechanism. (The Observed Population can contain components serving different functions).

G7 Manufacturer

Text (Compulsory)

G8 Observed population identification number

Numeric/optional

Numeric ID added in the case more than one observed population is entered - for same plant, system and type of component - that describe different OPs of components in the same system. G8 is added to "G0 Observed Population/CCCG identifier" to distinguish otherwise identical "G0 identifiers".

5. STATISTICAL RECORD FOR THE OBSERVED POPULATION/CCCG

S1 Component failure modes

Code/Compulsory

The components of the Observed Population/CCCG are part of a system or several systems. The components must perform certain functions that are necessary for the fulfilment of the system's function(s).

The failure mode field consists of the set of CCCG function failures the occurrence of each of which could prevent the system from fulfilling its function(s).

Only those failure modes are included for which component failures are collected.

The separate component coding guidelines contain the failure modes applicable to the specific components.

In general, few codes are sufficient to describe the possible failure modes of a given component.

S2 Number of Observed Populations/CCCGs

Not used. Default set to 1. Hidden in database system.

Numeric/Compulsory

Number of identical Observed Populations/CCCGs observed, default is 1. (generally, the entry is 1, except for twin plants)

S3 Start of observation time for Observed Population/CCCG

Date/Compulsory

Date of the first day of the evaluated time period for the Observed Population/CCCG.

Format: YYYY/MM/DD

S4 End of observation time for Observed Population/CCCG

Date/Compulsory

Date of the last day of the evaluated time period for the Observed Population/CCCG. Updated each time an evaluation of a further time period is added to the database.

Format: YYYY/MM/DD.

The total Observed Population/CCCG observation time can be calculated as (S4-S3)•S2.

S5 Number of independent failure events

Numeric /Compulsory

Given by independent counter (for each component failure mode listed in S1).

The same criteria must be applied for the recording of independent and dependent failures.

Each time the end of observation time (field S4) is updated; the independent failure count must be updated.

Depending on how the "Number of independent failures" is generated the following S5 flags shall be entered.

1. "Real" count - for specified CCCG, failure mode and observation time.

2. "Average" based on real count - for same type of component in plant series, failure mode and observation time.

3. "Estimated" based on generic failure rate - for same type of component in country including uncertainty.

S6 Exposure time

Numeric/optional

This field indicates or estimates exposure time. Depending on the failure mode in question the exposure time can be:

- cumulative time in standby per component or
- cumulative operational time per component

The format is hours.

S7 Demand cycles/number of demands

Numeric / optional

This field indicates the observed or estimated number of demand cycles for standby components, for example, number of cycles for a specific valve type.

Field S1 may need to be updated in rare cases in which CCF failure modes are observed that do not match any of the codes listed in field S1, see also the remark on field C3. Fields S4, S5 and eventually S6, S7 are updated each time the observation time is updated. The total number of Observed Population *(for all plants in all countries) and the corresponding total observation time, independent failure counts, numbers of demands, etc. are calculated in the ACCESS data base*

6. ICDE EVENT RECORD

The ICDE Event Record contains the Factual Event Description, C1-C6, and the Event Interpretation and System Influence, C7-C13.

A new ICDE Event Record is generated each time a new CCF event is added to the database. If an event occurs in several plants, separate records should be provided. A comment shall be included in the event description fields for the multiple unit events.

G0 Observed Population/CCCG identifier

Code/Automatic

See CCCG or EP identification record

C1 CCF event identifier

α-numeric/Compulsory

Unique identifier provided by the submitting country. The event code is a unique character string, used to identify each CCF event. The format may be "Ssss-Dddd-####", where Ssss is the source document/database in which the CCF event was identified, The Dddd portion is the plant's docket number. The #### portion is a sequential four digit event number.

C2 Date(s) of event(s)

Vector/Compulsory

The length of the vector is equal to the size of the Exposed population (field C4). The maximum latent time should be indicated, taking into account the test procedure and failure mode/cause.

Each vector component consists of the

- Date and time of detection of the event.
- The date of occurrence, expressed by "latent time". If the occurrence date is unknown, the earliest date it could have occurred should be indicated. Default is the previous test as given by the test interval.

Format:

	C2-1	**C2-2**
Event	Date(s) and time(s) of detection	Latent time (time from occurrence to detection)
1	YYYY/MM/DD HH/MM/SS	Days or fraction of days
2	YYYY/MM/DD HH/MM/SS	Days or fraction of days

C3 Failure mode

Code/Compulsory

The failure mode field describes the function the components failed to perform.

Only one code from field S1 is entered with the ICDE event record. For each failure mode a different CCF record is developed.

Example: loss of lubrication event for a pump. In most cases, the pump would start but eventually seize and fail. Therefore, the failure mode is failure to run. If the loss of lubrication prevents a successful start, for example, because of pump protection, the failure mode is failure to start.

For exceptional cases, a suitable code may not be found in field S1. Then, a new code has to be introduced and defined in S1, its independent failure count has to be included in field S5.

C4 Exposed population size

Numeric/Compulsory

This field indicates the size of the Exposed Population that is susceptible to the observed common cause failure event.

In most cases, this number will be the same as the Observed Population/CCCG size. However, as specific failure events may not affect all components of Observed Population the appropriate number can also be smaller than the Observed Population size (see definition in section 3.1).

C5 Event description

Text/Compulsory

The coding background shall be given. The text begins with a short description or title of the event, followed by a detailed factual description of the failure event, including all relevant circumstances, for example:

- system operating on demand, system in standby
- influences or causes introduced by test and maintenance activities or by external events
- method of discovery
- any special circumstances, environmental conditions
- operational state of the plant at the time the event was discovered. The power field contains the power level at the time of the CCF event as a percentage of full power.
- description of the observed damage to the component
- characterisation of the condition that is readily identifiable as leading to the failure
- description of causes
- conditioning event
- trigger event

- if detected by test: type of test and test interval
- operative action
- time in failed state (time to detection, if known, time to repair)
- reference to equal or similar events at other units/plants. This is to indicate to an analyst that there may be a coupling of events at different units/plants, for example, by weather conditions
- time from actuation to failure to run
- corrective action

As the factual event description forms the basis for the event interpretation it has to be as clear and complete as possible.

C6 Detection

Vector/Compulsory

Length of the vector is equal to the size of the Exposed population (field C4)

The following coding is suggested:

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/TA/TL	test during operation/annual overhaul/ laboratory.
TU	unscheduled test
U	unknown

C7 CCF event interpretation

Text/Compulsory

Description of the (subjective) rationale used by the analyst to classify the event as a CCF event, for example:

- failure mechanism,
- root cause,
- safety implication for the system or function in question,
- applicability to other operational states,
- safety implication for other plants.

C8 Component impairment vector

Vector/Compulsory

The length of the vector is equal to the size of the Exposed population (field C4).

Information on the impairment status of each component of the Exposed population. The following coding is suggested:

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

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

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

If parts were replaced on some components due to failures of parallel components, this code is used for the components that didn't actually experience a failure. This also applies if it was decided to implement said replacement at a later time.

W - Working. The component is working according to specifications.

There must be as many impairment attributes as the CCCG or EP size in field C4. The default attribute is "W" indicating no impairment. A potential impairment (e.g., a design flaw that would have resulted in failure) will be coded as actual impairment if it is certain that the degradation would have occurred. For example, a wiring discrepancy that would have prevented a pump start is coded as complete failure, because it is certain that the pump would not have started. If the CCF event only affected two of three pumps, the coding is $C_1 = C_2 = C$, $C_3 = W$.

Comparison to the numerical coding used by NRC

C	*D*	*I*	*W*
p=1	*p=0.5*	*p=0.1*	*p=0*

C9 Root cause

Code/Compulsory

The cause field identifies the most basic reason for the component's failure. Most failure reports address an immediate cause and an underlying cause. For this project, the appropriate code is the one representing the

common cause, or if all levels of causes are common cause, the most readily identifiable cause. The following coding is suggested:

C - state of other component(s) (if not modelled in PSA)

The cause of the state of the component under consideration is due to the state of another component. Examples are loss of power and loss of cooling.

D - design, manufacture or construction inadequacy

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

A - abnormal environmental stress

Represents causes related to a harsh environment that is not within component design specifications. Specific mechanisms include chemical reactions, electromagnetic interference, fire/smoke, impact loads, moisture (sprays, floods, etc.) radiation, abnormally high or low temperature, vibration load, and severe natural events.

H - human actions

Represents causes related to errors of omission or commission on the part of plant staff or contractor staff. An example is a failure to follow the correct procedure. This category includes accidental actions, and failure to follow procedures for construction, modification, operation, maintenance, calibration, and testing. This category also includes deficient training

M – maintenance

All maintenance not captured by H - human actions or P - procedure inadequacy.

I - internal to component, piece part

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

P - procedure inadequacy

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

O - other

The cause of events is known, but does not fit in one of the other categories in the classification scheme.

U – unknown

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

C10 Coupling factor(s)

Code/Compulsory

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. The following coding is suggested:

H - Hardware (component, system configuration, manufacturing quality, installation configuration quality).

Coded if none of or more than one of HC, HS or HQ applies, or if there is not enough information to identify the specific “hardware” coupling factor.

HC - hardware design

Components share the same design and internal parts

HS - system design

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

HQ- hardware quality deficiency

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

O – Operational (maintenance/test (M/T) schedule, M/T procedures, M/T staff, operation procedure, operation staff).

Coded if none of or more than one of OMS, OMP, OMF, OP or OF applies, or if there is not enough information to identify the specific “maintenance or operation” coupling factor.

OMS - maintenance/test (M/T) schedule,

Components share maintenance and test schedules. For example, the component failed because maintenance was delayed until failure.

OMP - M/T procedure

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

OMF - M/T staff

Components are affected by a maintenance staff error.

OP - operation procedure

Components are affected by an inadequate operations procedure. For example, the component failed because the operational procedure was incorrect and the pump was operated with the discharge valve closed.

OF - operation staff

Components are affected by the same operations staff personnel error.

E - Environmental (internal, external)

Coded if none of or more than one of EE or EI applies, or if there is not enough information to identify the specific "environmental" coupling factor.

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.

C11 Shared cause factor

Code

By definition, a CCF event must result from a single shared cause of impairment. However, the failure reports may not provide sufficient information to determine whether the multiple impairments result from the same cause or different causes. Because of this lack of detailed description of the causes in the event reports, the analyst must make a subjective assessment about the potential of a shared cause. The shared cause factor allows the analyst to express his degree of confidence about the multiple impairments resulting from the same cause. The codes High, Medium, Low, No are used. Examples are the following:

<u>High</u>

This code is used when the analyst believes that the cause of the multiple impairments is the same, regardless of the cause. A shared-cause factor code "High" implies multiple impairments from the same root cause of impairment, often resulting in the same failure/degradation mechanism and affecting the

same piece-parts of each of the multiple components. The corrective action(s) taken for each of the multiple components involved in the event typically is (are) identical.

Example:

"Three check valves in the turbine steam-supply line failed to open. Investigation revealed similar internal damage to all three valves. The cause of impairment for each valve was steam system flow oscillations causing the valve discs to hammer against the seat. The oscillations were ultimately attributed to inadequate design. The valve internals were replaced, and a design review is being conducted to identify ways of reducing flow-induced oscillations."

Statements in the event report that indicate the same cause, failure mechanism, or failure symptoms are usually good indicators of a shared cause of impairment. This is true even if little information is provided about the exact nature of the problem.

The following examples illustrate such statements:

"Investigation revealed similar damage to all three redundant valves" "loose screws found in five circuit breakers" "several air-operated valves malfunctions because of moisture in the air supply".

If the event report contains no information about the causes of impairment, the analyst should use the code "High". To change this code requires evidence or an indication that the causes were different. This evidence need not come from the event description itself, but may result from a more general knowledge of the plant and its operational history.

Medium

This code is used when the event description does not directly indicate that multiple impairments resulted from the same cause, involving the same failure mechanism, or affected the same piece-parts, but there is strong evidence that the underlying root cause of the multiple impairments is the same.

Example:

"Binding was observed in two check valves. Wear of the hinge pin/pin bearing is suspected to have caused the binding of the valve disc, resulting in impairment of the first valve. The hinge pins were binding in the second valve due to misalignment. Further investigation of the second valve impairments revealed inadequate repair/maintenance instructions from the vendor and engineering department."

The event description presents two different causes of impairment (wear and misalignment) for these valves. Therefore, these failures could be considered independent. However, it is clear that there is a programmatic deficiency associated with repair/maintenance of these valves. It is possible, for example that the inadequate instructions from the vendor/engineering department resulted in the first valve being misaligned and the misalignment caused abnormal or excessive wear. It is also possible that the event descriptions were written by different people, and the difference in the cause description is simply a difference in their writing styles (one focused on the actual cause [misalignment], the other on the symptom [wear]). In either case, both valves would have failed because of misalignment, making this a CCF.

Low

This code is used when the event description indicates that multiple impairments resulted from different causes, involved different failure mechanisms, or affected different piece parts, but there is still some evidence that the underlying root cause of the multiple impairments is the same.

Example:

“Water was found in the lubricating oil for the motor of the RHR “D” pump. The source of the water was a loose fitting at the motor cooling coil. The fitting was replaced.”

“A severe seal water leak was observed at the RHR 'B' pump. The source of this leak was a missing ferrule in the seal water line purge fitting. The ferrule was possibly left out during previous pump seal repairs. A new pump seal fitting ferrule was installed.”

These events involved different pump sub-components (motor cooling and seal water), and the specific causes of impairment are different (loose fitting and missing ferrule). These are indications that the impairments are independent. However, it can also be speculated that the utility has programmatic deficiencies (e.g., inadequate training and procedures) regarding water piping connections and fittings, particularly if there has been a history of similar events. If so, the root cause of the problem is lack of training, inadequate procedures, etc., thereby making the cause of the multiple impairments the same. Since this hypothesis is highly speculative, the shared-cause factor is “Low”.

No

This code is used when the analyst believes that the multiple impairments resulted from clearly different causes. (This value is rarely used because events with shared-cause code “No” are typically not included in the CCF database.)

Comparison to the numerical coding used by NRC

high	*medium*	*low*	*no*
p=1	*p=0.5*	*p=0.1*	*p=0*

C12 Corrective actions

Code/Compulsory

This field describes the actions taken by the licensee to prevent the CCF event from re-occurring. The defence mechanism selection is based on an assessment of the root cause and/or coupling factor between the impairments. The following coding is suggested:

A - general administrative/procedure controls

Administrative control or a procedure control.

B - specific maintenance/operation practices

Specific maintenance or operational practice.

C - design modifications

Design modification.

D - diversity

Addition of diversity. This includes diversity in equipment, types of equipment, procedures, equipment functions, manufacturers, suppliers, personnel, etc.

E - functional/spatial separation

Modification of the equipment barrier (functional and/or physical interconnections). Physical restriction, barrier, or separation.

F - test and maintenance policies

Maintenance program modification. The modification includes items such as staggered testing and maintenance/operation staff diversity.

G - fixing of component

O - other

The corrective action is not included in the classification scheme.

U - Unknown

Adequate detail is not provided to make an adequate corrective action identification.

C13 Coding justification

Text/optional
This field is for the analyst's comments and assumptions on coding decisions. For example, if there are two different failure modes for two impairments within the CCF event, the second failure mode would be discussed here, even though an additional record was created for the second failure mode. For CCF events identified from LERs, the LER number is referenced here.

C14 Time factor

Code/Compulsory

This is a measure of the "simultaneity" of multiple impairments. The attribute of the time factor (see below) is determined by the time between detection of individual impairments. In general, a weighting factor is assigned to the CCF event based on the time between individual impairments. The acceptable input for this field can be a decimal number from 0.1 to 1.0. The applied values depend on PRA mission time, failure mode, operating conditions, testing schemes and TechSpec instructions on how to proceed after detection of a failed component. As some of these items differ in different plants and systems, it is not possible to generally account for them in the data collection. Therefore, tailoring of events for building PRA data sets may need a reassessment of time factor values.

Specific time factor attributes and values to be used for some common scenarios are:

Failure to run/operate of operating components and stand-by components in operating mode(s)

High: Multiple component impairment occurring within PRA mission time. The weight factor is 1.0.

Medium: Multiple component impairment occurring outside PRA mission time, but within a one month's period (for operating components) or within double mission time (for stand-by components). The weight factor is 0.5.

Low: Multiple component impairment occurring more than one month apart (for operating components) or more than double mission time (for stand-by components). The weight factor is 0.1.

Remark: for stand-by components operating times have to be summed up from running times during tests and operational demands

Other failures (to start, stop, switch of position etc.) of stand-by components and operating components with cyclical change of operation time (i.e. at a given time only x of n components are operating, with cyclical change)

High: Multiple component impairment discovered during testing or by observation within one test cycle of length T (test cycle T is the time between two consecutive tests of one component). The weight factor is 1.0

Medium: Multiple component impairment discovered during testing or by observation within two subsequent test cycles (length 2T), the events being separated by at least T. The weight factor is 0.5.

Low: Multiple component impairment discovered during testing or by observation two test cycles apart (at time 2T). The weight factor is 0.1.

Exceptions: There may exist conditions such as

- TechSpecs requirements to test all components of a system immediately after inoperability is detected,
- Other operational demands within test cycle etc. that would make it appropriate to reduce T to e.g. T/2

Impairments separated by more than twice the test interval (i.e. after the initial detection of an impairment of a component in the observed population a further component is detected to be failed after it was successfully tested at least twice under conditions appropriate for detecting the respective impairment), or by more than a scheduled outage period, will not be included.

Examples:

- Recurrent testing of one component reveals a complete failure of the component (impairment “C”) or a significant degradation (impairment “D”). Subsequent inspection of redundant components reveals an incipient impairment of a further component (impairment “I”). Time factor is high because both impairments were detected at the same time.

- Recurrent testing of one component reveals a complete failure of the component (impairment “C”). Two test cycles later a redundant component fails due to the same cause (impairment “C”). Time factor is low because both failures were detected two test cycles apart.

- Failure or degradation of one or more components is detected by inspection and repaired. As precautionary measure it is decided to replace parts at other components. The impairment code “I” is used for the components that did not actually experience a failure. The time factor is “high” because the detection of the failure or degradation and the decision to consider other components as incipiently degraded occur within short time. This also applies if it was decided to implement said replacement at a later time.

7. LISTING OF OTHER DOCUMENTS REFERENCED IN THE ICDE FORMAT DEFINITION

Joint IAEA/NEA IRS guidelines. NEA/CSNI/R(1997)12. 1997.

T-Book. Reliability data from the Nordic power reactors, Version 5. Vattenfall / Swedpower, Sweden. 2000.

Common Cause Failure Data Collection and Analysis System: Overview, Vol. 1, NUREG/CR-6268. US NRC. June 1998.

ANNEXES ICDE CG 01-06

ICDE

International Common-Cause-Failure Data Exchange **ICDECG01**

Title:	Coding Guidelines for centrifugal pumps
Author(s):	Wolfgang Werner, Gunnar Johanson
Issued By:	Gunnar Johanson
Reviewed By:	WG
Approved By:	
Abstract:	This report defines the component specific coding rules for centrifugal pumps
Doc.ref:	Coding Guidelines
Distr.	WG, Project Web Site, Project archive

Revision control:	Version	Date	Initial
	Draft 1.1		
	Draft 1.2	Functional failure modes added	MC
	Draft 1.3	1998-10-19	GJ
	Draft 2	1999-01-13	
2001-02-12	Draft 2.1	Change of old definitions in the part Coding Rules and Exceptions	EJ
2003-02-10	Draft 2.2	Addition of functional failure modes so that guideline and database corresponds.	EJ
2003-04-24	Draft 2.3	Deletion of the added failure modes	EJ
2003-10-17	Draft 2.4	Updates in the part Coding Rules and Exceptions.	EJ

COMPONENT CODING GUIDELINES FOR CENTRIFUGAL PUMPS

General Description of the Component

This family of pumps is comprised of those centrifugal pumps (CP) that are motor driven and are used for the purpose of establishing flow to or from the primary system or support systems.
Centrifugal pump data are being collected for the systems:

- auxiliary/emergency feedwater
- high pressure safety injection (PWR)
- low pressure safety injection, including residual heat removal (PWR)
- containment spray
- ice condenser
- high pressure coolant injection/reactor core isolation cooling (BWR)
- low pressure coolant injection, including residual heat removal (BWR)
- component cooling, including reactor building closed cooling water
- essential SWS
- essential raw cooling water
- standby liquid control (BWR)
- emergency power generation and auxiliaries, including supply of fuel and lubrication oil.

For data evaluation purposes, the family of centrifugal pumps is subdivided into six subgroups characterised by pump delivery head and mass flow rate. The classification is shown in table 1.

Component Boundaries

The component for this study is the centrifugal pump, comprised of a pump with its internal piece-part components and a driver. The driver includes the circuit breaker, power leads, local protective devices, open/close limit switches, torque switches, and the motor. The control circuit that induces a start and stop signal to a CP is not included within the CP boundary if it also controls other component functions, such as other pump actions, opening or closing of valves, etc.

Event Boundary

The mission for a CP is to maintain the water inventory in the primary system, or to maintain cooling flow in the primary or secondary system or in support systems.

Some of the systems for which CP data are being collected serve dual purposes (low pressure injection and residual heat removal), such that the flow paths are also used during normal plant operation.

Failure of the CP to perform its mission occurs if a pump that is required to be running to allow injection or cooling flow fails to start or fails to run.

Basic unit for ICDE event collection

The basic set for centrifugal pump data collection is the "common-cause component group", (CCCG: set of identical components in a system, performing the same function). The CCCG size typically varies from two to twelve, with the bulk ion the two to four range.

Time frame for ICDE event exchange

The minimum period of exchange should cover a period of 5 years (The initial pump exchange cover Jan. 1 1990 - Dec. 31 1994, ref. Park City protocol).

Coding Rules and Exceptions

1. In general, the definition of the ICDE event given in section 2 of the General ICDE Coding Guidelines applies.
2. Some reports discuss only one actual failure, and do not consider that the same cause will affect other CPs, but the licensee replaces the failed component on all CPs as a precautionary measure. This type of event will be coded as incipient impairment (0.1) of the components that did not actually fail.
3. In-operability due to seismic criteria violations will not be included, unless an actual failure has occurred.
4. Administrative in-operability that does not cause the pump to fail to function was not included as failures. An example is a surveillance test not performed within the required time frame.
5. Failure of the electrical operator without coincident failure of the manual operator is considered a CP failure.
6. In-operability due to human error or erroneous calibration/set up will be included (in either ICDE or independent event coding).
7. All actual failures will be included (in either ICDE or independent event coding), even if the event report considers them to be invalid.

Functional Fault Modes

1. Failure to start: failure before nominal operating conditions is reached (FS).
2. Failure to run: failure after nominal operating conditions has been reached (FR).
3. Failure to stop/close (FC)
4. Internal leakage (IL)
5. External leakage (EL)

Table 1. Definition of centrifugal pump subgroups by ranges of pump delivery head and mass flow rate.

	<75 kg/s Small Flow	>75 kg/s Large Flow
0.2-2 Mpa Low pressure	Centrifugal pumps, Low pressure Small flow, horizontal and vertical CP- LS -OP- operational (T-book Table 1) CP- LS -Int- intermittent CP- LS -SB- Standby CP- LS -TD- turbine driven	Centrifugal pumps, Low pressure Large flow, horizontal and vertical CP-LL-OP- operational (T-book Table 2), (T-book Table 3) CP-LL-Int- intermittent (T-book Table 5a) CP-LL-SB- Standby CP-LL-TD- turbine driven (T-book Table 9)
Example system	Cooling and cleaning system for spent fuel Service water system Heating system	Salt water system Secondary cooling system System for contaminated waste water, ion exchanger Refuelling water storage Service water system Residual heat removal system (PWR) Containment spray system LP Safety injection system BWR LP Core spray system BWR
2-8 Mpa Medium pressure	Centrifugal pumps, Medium pressure Small flow, horizontal and vertical CP-MS-OP- operational CP-MS-Int- intermittent CP-MS-SB- Standby (T-book Table 7) CP-MS-TD- turbine driven (T-book Table 9)	Centrifugal pumps, Medium pressure Large flow, horizontal and vertical CP-ML-OP- operational CP-ML-Int- intermittent CP-ML-SB- Standby (T-book Table 8) CP-ML-TD- turbine driven
Example system	Auxiliary feed-water system PWR Emergency (Auxiliary) feed-water system BWR Residual heat removal system (TVO)	HP Safety injection system BWR
8-20 Mpa High pressure	Centrifugal Pumps, High pressure Small flow, horizontal and vertical CP-HS-OP- operational CP-HS-Int- intermittent CP-HS-SB- Standby (CP-HS-TD- turbine driven)	Centrifugal pumps, High pressure Large flow, horizontal and vertical CP-HL-OP- operational CP-HL-Int- intermittent (T-book Table 5b) CP-HL-SB- Standby CP-HL-TD- turbine driven

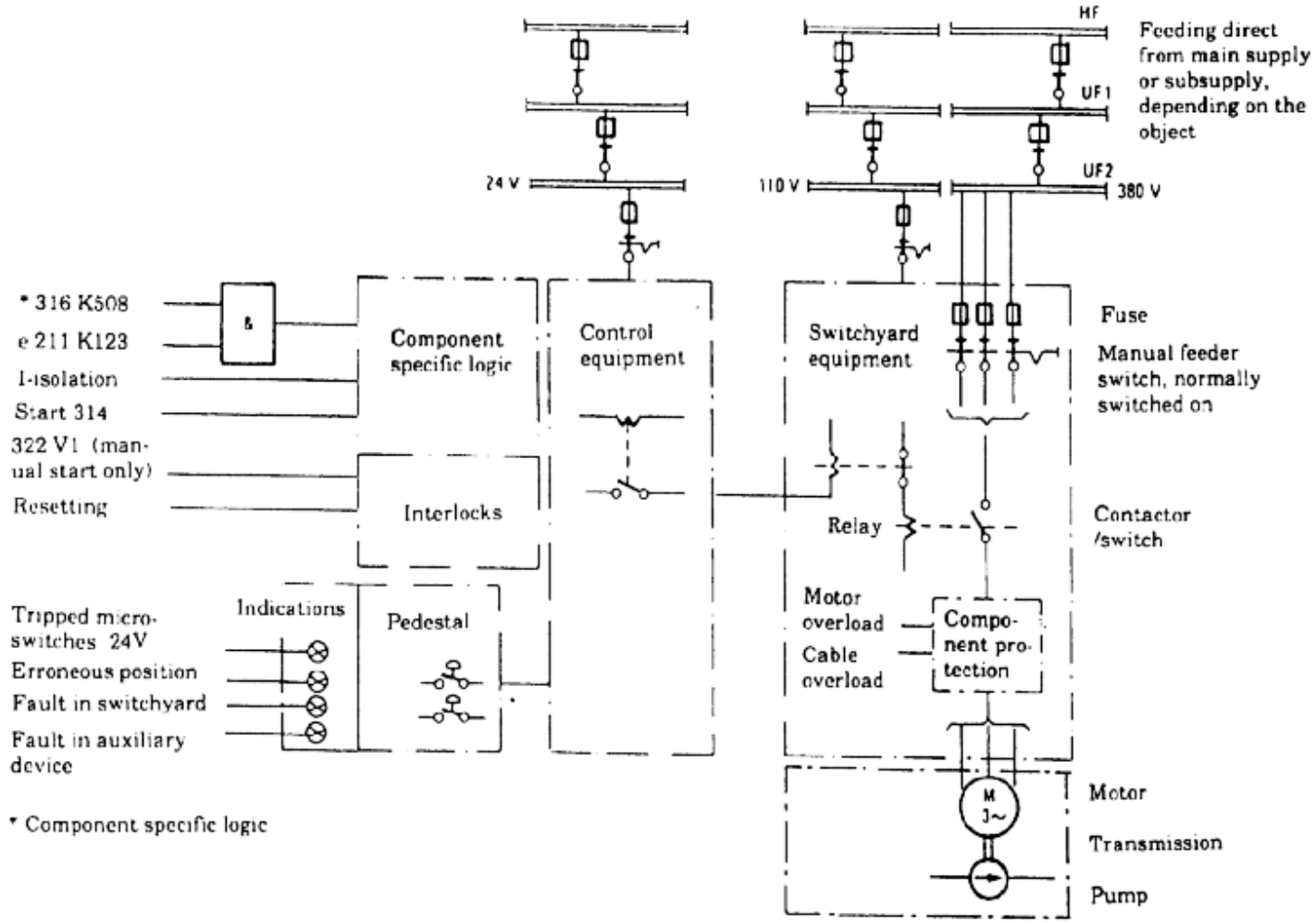


Figure 1. Physical boundary of centrifugal pumps

ICDE

International Common-Cause-Failure Data Exchange **ICDECG02**

Title:	Coding Guidelines for Motor- Operated Valves
Author(s):	Dale Rasmuson, Wolfgang Werner, Gunnar Johanson, Esther Jonsson
Issued By:	Gunnar Johanson, Marina Concepcion
Reviewed By:	WG
Approved By:	
Abstract:	This report defines the component specific coding rules for Motor- Operated Valves
Doc.ref:	Coding Guidelines
Distribution	WG, Project Web Site, Project archive

Revision control:	Version	Date	Initial
1998-03-16	Draft 1.1	Initial proposal	DR
1999-05-10	Draft 1.2	Corrections following the Paris meeting CCW added and exposed population def. corrected. Component types added, Failure modes added	GJ, MC
2001-02-12	Draft 2.0	Change of old definitions in the part Coding Rules and Exceptions	EJ
2001-11-20	Draft 2.1	Change of incorrect sentence under the section “Basic unit for ICDE event collection”.	EJ

CODING GUIDELINES FOR MOTOR-OPERATED VALVES

General Description of the Component

This family of valves is comprised of those emergency core cooling system (ECCS) valves that are motor operated and are used for the purpose of establishing or isolating flow to or from the primary system. The systems for which motor operated valve (MOV) data are collected are:

- auxiliary feedwater
- high pressure safety injection
- low pressure safety injection (residual heat removal)
- refuelling water storage tank
- containment spray
- pressurizer power operated relief valve block valves
- high pressure coolant injection/reactor core isolation cooling (BWR)
- low pressure coolant injection (residual heat removal) (BWR)
- isolation condenser (BWR)
- component cooling water
- essential SWS

The following component types are distinguished:

- MOV Ball valve
- MOV Gate valve
- MOV Globe valve
- MOV Butterfly valve
- MOV General type

Component Boundaries

The component for this study is the MOV, comprised of a valve with its internal piece-part components and a motor operator. The operator includes the circuit breaker, power leads, local protective devices, open/close limit switches, torque switches, and the motor. The control circuit that induces a close or open signal to an MOV is not included within the MOV boundary if it also controls other component functions, such as other valve actions, pump starts, etc. (Compare figure 1).

Event Boundary

The mission for an MOV is to allow flow of water into the primary system following a LOCA or to prevent water from leaving the primary containment system in the event of a LOCA. Some of the systems for which MOV data were reviewed serve dual purposes (low pressure injection and residual heat removal), such that the flow paths are used during normal plant evolutions. Failure of the MOV to perform its PRA mission occurs if a valve that is required to be open to allow injection or cooling flow does not

open, or if a valve that is required to close to isolate secondary parts of the ECCS after a LOCA fails to close.

Basic unit for ICDE event collection

The basic set for motor operated valve data collection is the "exposed population" (EP: set of components exposed to the same failure mechanism). The number of valves in an exposed population depends on the specific failure identified in the event analysis.

In general the exposed population shall be in the same system for the components identified but could be modified depending on the linkage of CCF events by failure mechanism or causal factors.

The elements of the exposed population will normally have similar test intervals. Similar in this context means a factor of not more than 2 between minimum and maximum.

The determination of the exposed population is left to the event reviewer and the reviewer's knowledge of the relation of system design, operation and testing.

Time frame for ICDE event exchange

The minimum period of exchange should cover a period of 5 years (The initial pump exchange cover Jan. 1 1990 - Dec. 31 1994, ref. Park City protocol).

Coding Rules and Exceptions

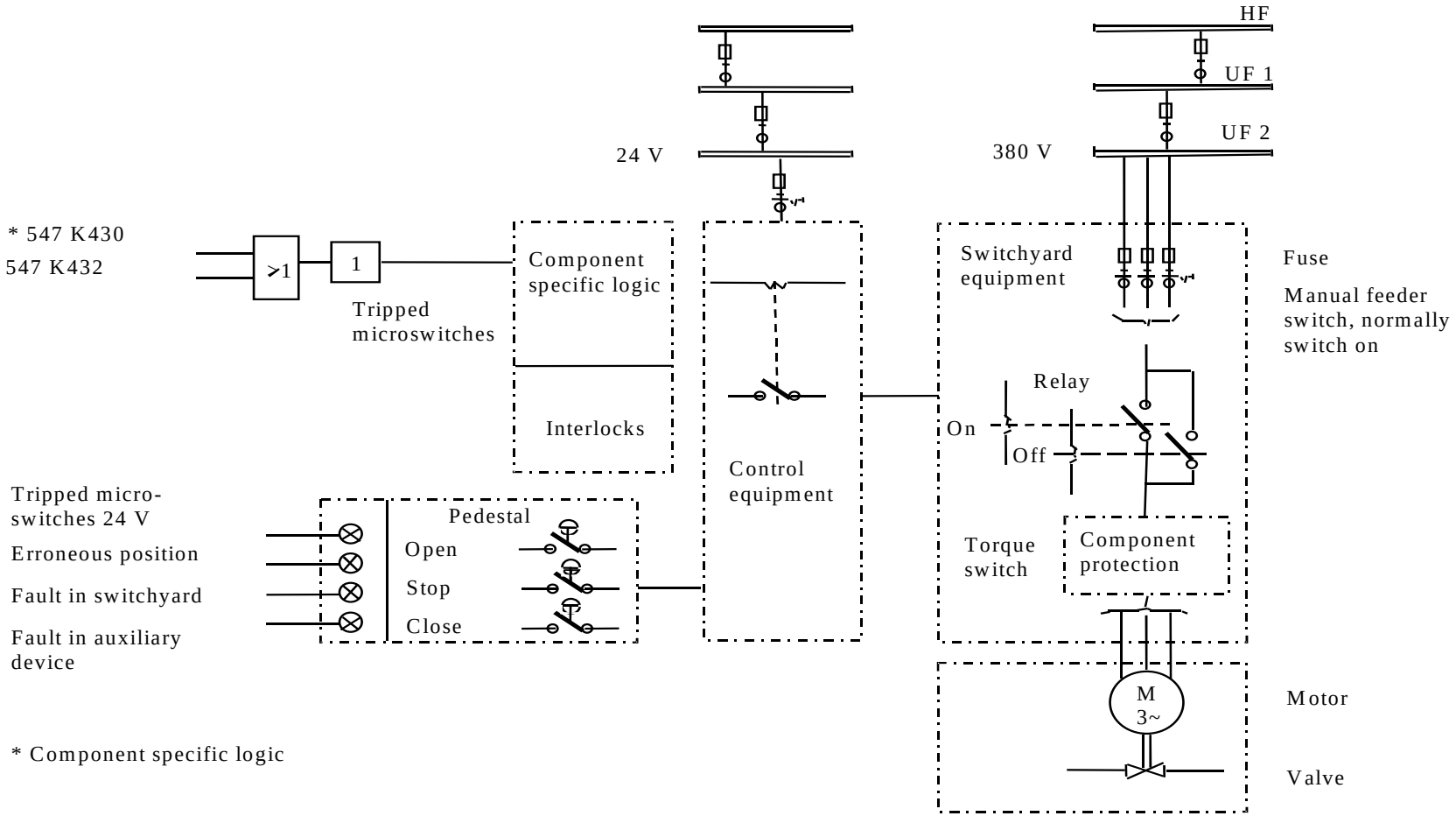
1. In general, the definition of the ICDE event given in section 2 of the General ICDE Coding Guidelines applies.
2. Some reports discuss only one actual failure, and do not consider that the same cause will affect other MOVs, but the licensee replaces the failed component on all MOVs as a precautionary measure. This type of event will be coded as incipient impairment (0.1) of the components that did not actually fail.
3. In-operability due to seismic criteria violations will not be included, unless an actual failure has occurred.
4. Administrative in-operability that does not cause the valve to fail to function was not included as failures. An example is a surveillance test not performed within the required time frame.
5. Failure of the electrical operator **without coincident failure of the manual operator** is considered a MOV failure.
6. Failure of the MOV to cycle in the required time (as opposed to mission time) will not be considered a failure, either CCF or independent, if the MOV reached its intended state.

Functional Fault Modes

1. Failure to open (FO)
2. Failure to close (FC)
3. Internal Leakage (IL)
4. External Leakage (EL)

Component boundaries (next page)

Figure 1. The schematic diagram shows the component boundaries for MOVs.


HF
UF 1
UF 2
24 V
380 V
* 547 K430
547 K432
>1
1
Tripped microswitches
Component specific logic
Interlocks
Control equipment
Switchyard equipment
Fuse
Manual feeder switch, normally switch on
Relay
On
Off
Torque switch
Component protection
Tripped micro-switches 24 V
Erroneous position
Fault in switchyard
Fault in auxiliary device
Pedestal
Open
Stop
Close
M
3~
Motor
Valve
* Component specific logic

ICDE

International Common-Cause-Failure Data Exchange **ICDECG03**

Title:	Coding Guidelines for Emergency Diesel Generators
Author(s):	Dale Rasmuson, Wolfgang Werner, Gunnar Johanson
Issued By:	Gunnar Johanson , Marina Concepcion
Reviewed By:	WG
Approved By:	WG
Abstract:	This report defines the component specific coding rules for Emergency Diesel Generators
Doc.ref:	Coding Guidelines
Distribution	WG, Project Web Site, Project archive

Revision control:	Version	Date	Initial
	Draft 2	1999-01-13	GJ

CODING GUIDELINES FOR EMERGENCY DIESEL GENERATORS

General Description of the Component

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

Component Boundaries

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

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

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

Event Boundary

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

Basic unit for ICDE event collection

The basic set for centrifugal pump data collection is the "common-cause component group", (CCCG: set of identical components in a system, performing the same function). The CCCG size typically varies from two to eight, with the bulk ion the two to four range.

Time frame for ICDE event exchange

The minimum period of exchange should cover a period of 5 years (The initial pump exchange cover Jan. 1 1990 - Dec. 31 1994, ref. Park City protocol).

Coding Rules and Exceptions

1. High-pressure core spray (HPCS) diesels will be included as a separate train of the emergency AC power system. They do not have sequencers, but usually the EDG component itself is very similar to the main EDGs.
2. Swing EDGs will be considered to belong to each unit of a multiple unit site, such that a failure of the swing EDG will affect each unit.
3. In general, the definition of the ICDE event given in section 2 of the General ICDE Coding Guidelines applies.
4. Some reports discuss only one actual failure, and do not consider that the same cause will affect other EDGs, but the licensee replaces the failed component on all EDGs as a precautionary measure. This will be coded as incipient impairment (0.1) of the components that did not actually fail.
5. Failures that occur in equipment that is not needed for emergency actuation (e.g. test circuitry) will be coded as incipient component impairment (0.1)
6. Inoperability due to seismic or electrical separation criteria violations will not be included, unless an actual failure has occurred.
7. Inoperability due to administrative actions will not be included as a failure if the report states that the G could have started on an emergency signal. (Example: a surveillance test not performed within the required time frame.)
8. Troubleshooting start attempts that result in equipment failures will not be counted if the failed equipment is what initiated the maintenance and troubleshooting sequence. If there is a failure on the operational surveillance test following maintenance on equipment other than what was being fixed, another failure will be counted.

Functional Failure Modes

1. Failure to start (FS). A successful start will be the ED/EDG start through breaker closing and full sequence of loading. If the start is a test that requires no loading, the success criteria will be only the /EDEDG start. Failure to start in the required time (per test procedures) will not be considered a failure, unless the ED/EDG did not start prior to actuation of the "fail to start" relay and subsequent termination of the start sequence.
2. Failure to run (FR.). The /EDEDG must be loaded (required for the current conditions) and stable prior to the failure.
3. Failure to stop (FC).

ICDE

International Common-Cause-Failure Data Exchange **ICDECG04**

Title: Coding Guidelines for Safety Valves/Relief Valves

Author(s): Dale Rasmuson, Wolfgang Werner, Gunnar Johanson

Issued By: Gunnar Johanson, Marina Concepcion

Reviewed By: WG

Approved By: WG

Abstract: This report defines the component specific coding rules for Safety Valves/Relief Valves

Doc.ref: Coding Guidelines

Distribution WG, Project Web Site, Project archive

Revision control:

Version	Date	Initial
Draft 1.5	1999-05-10, Corrections following the Paris meeting Revised component classification.	GJ
Draft 1.6	2000-05-01, Clarification failure mode example	GJ
Draft 1.7	2000-10-06, Update of component types so that they can be used for Magnox and AGR.	EJ
Draft 1.8	2002-10-02 Editorial	GJ

COMPONENT CODING GUIDELINES FOR SAFETY VALVES/RELIEF VALVES

General Description of the Component

The function of the Safety Valves/Relief Valves (SV/RV) is to prevent overpressure of the components and system piping. The systems for which SV/RV are installed in and data are collected for are:

- Steam generators discharge headers (PWR, AGR, Magnox)
- Pressurizer vapour volume (PWR)
- Reactor coolant system, main steam headers (BWR, AGR, Magnox)

Safety Valves/Relief Valves component types are the following:

- Pressurizer power operated relief valves (PWR)
- Pressurizer 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 valves (BWR)
- Primary-Side safety valves (BWR, AGR, Magnox)

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 main steam headers SV/RV are exemplified in figure 1.1. As shown can the function be combined therefore are the following component sub-types defined for detailed classification, optional.

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

Event Boundary

Successful operation of a SV/RV is defined as opening in response to system pressure exceeding a predefined threshold, and re-closing when pressure is reduced below a predefined threshold. Note: 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.

Basic unit for ICDE event collection

The basic set for SV/RV data collection is the "common-cause component group", (CCCG: set of identical components in a system, performing the same function). The CCCG size typically varies from two to twelve.

Time frame for ICDE event exchange

The minimum period of exchange should cover a period of 5 years

General Coding Rules and Exceptions

1. All actual failures will be included (in either ICDE or independent event coding), even if the event report considers them to be "invalid."

2. Some reports discuss only one actual failure, and do not consider that the same cause will affect other SV/RVs, but the licensee replaces the failed component on all SV/RVs as a precautionary measure. This type of event will be coded as a CCF, with a low (0.1) component degradation value for the components that did not actually fail.

3. In-operability due to seismic criteria violations will not be included.

Functional Failure Modes

SV/RV malfunctions are defined as failures to open or close on demand, and failure to stay closed, including excessive leakage through the valve, or spurious opening of the valve. The failure modes used in evaluating the data are:

1. Failure to Open (FO): Examples are: SV/RV sticks closed or whenever a SV/RV is blocked shut.

Examples partial failures:

- SV/RV e.g. set point over 10% over the limit or some level that does not compromise the safety function, e.g. 10%.

- If piece-part(s) are replaced to calibrate a set point that was too high.

- Stroke time test failure will be considered a partial failure if it opening time is reported as “excessive”, otherwise it is not a failure.

2. Failure to Close (FC): Examples are: SV/RV stays open when it should close**,** SV/RV doesn't fully close.

3. Inadvertent opening (IO). Examples are: spurious opening. Leakage past the valve seats, and if piece-part(s) is replaced to re-calibrate a set point that was too low.

Valve operator failures are evaluated to determine the effect on valve operability. In general, if the failure causes the valve to fail to operate, it will be considered a valve failure.

Enclosure: Component picture of safety / relief valves

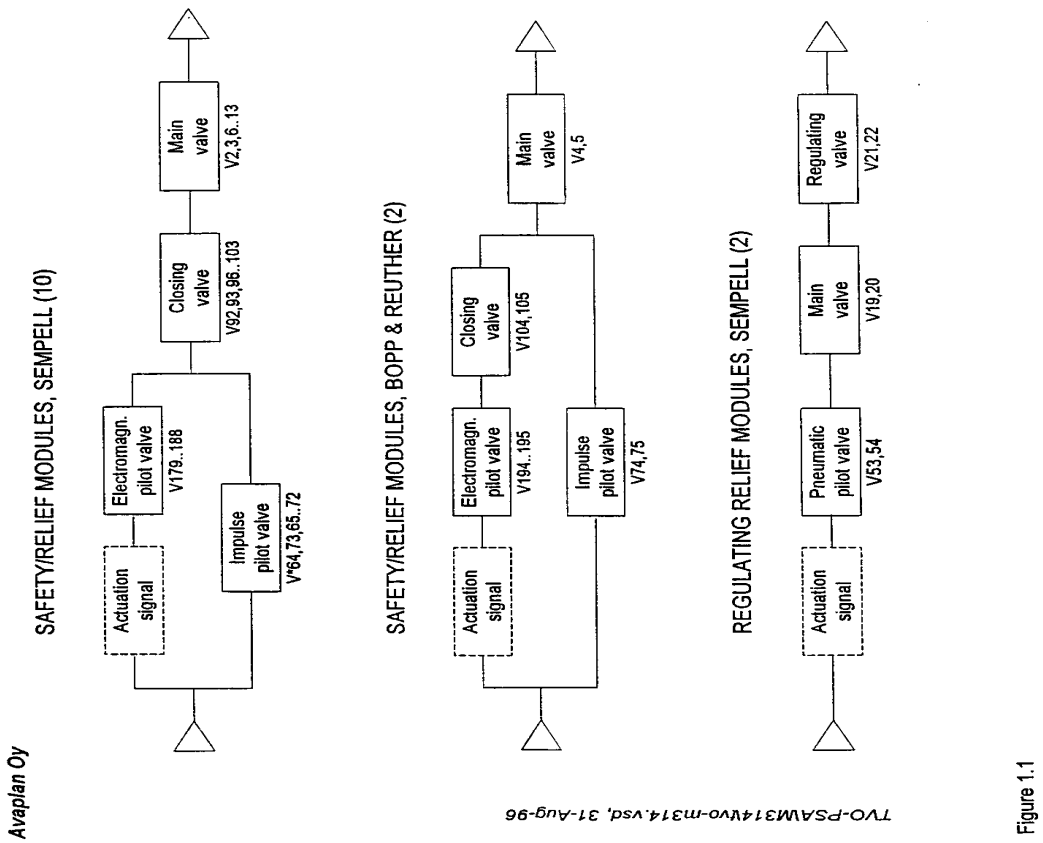


Figure 1.1

ICDE

International Common-Cause-Failure Data Exchange **ICDECG05**

Title:	Coding Guidelines for Check Valves
Author(s):	Dale Rasmuson, Wolfgang Werner, Gunnar Johanson
Issued By:	Wolfgang Werner, Marina Concepcion
Reviewed By:	WG
Approved By:	WG
Abstract:	This report defines the component specific coding rules for Check valves
Doc.ref:	Coding Guidelines
Distr.	Project archive

Revision control:

Version	Date	Initial
Draft 1.2	Components types; failure modes	MC
Draft 1.3	1999-05-03, Corrections following the Paris meeting	GJ
Draft 1.4	1999-07-08 Component types details	MC
Draft 1.5	2000-05-15 Clarifications, rules and exemptions	GJ
Draft 1.6	2000-10-18 Enclosure – Figures are included	EJ

CODING GUIDELINES FOR CHECK VALVES

General Description of the Component (codes G1, G4)

Check valves are used for the purpose of establishing or isolating flow to or from the fluid system. It is comprised of a valve with its internal piece-part components. The function of the check valve is to form a conditional boundary (i.e., one direction) between high pressure and low-pressure sections of a system during static conditions. By design, the valve will open to allow flow when the low-pressure section has experienced a pressure increase (e.g., pump start). This component is operated by system pressure overcoming gravity. Typically, there is no capability to manually open, close, or isolate these valves, however, some check valves have manual handwheels or levers (stop-check) and can be manually closed. Some check valves are "air-testable" which should not affect normal component operation and in some cases the air supply is turned off during operation as a precaution. No power is normally required for valve operation. Check valves are installed in systems in the following areas:

- Pump discharge,
- Pump suction,
- System inter- or cross-connection, and
- Pump turbine steam inlet.

The following component classification is proposed (G4):

- Swing check valve
- Lift check valve
- General type

The following details about component can be included in general description (G1):

Functional features:

- *CKA (air testable)*
- *CKB (vacuum breaker)*
- *CKS (stop check)*
- *CKV (check) depending on the valve design under consideration.*

More detailed type specification:

- *Butterfly swing check valve*
- *Horizontal lift check valve*
- *Damped check valve*

- *Flat poppet check valve*
- *Cone poppet check valve*

Systems included in the collection (codes G1, G3)

The systems for which check valve (CKV) data are collected are (G3):

- auxiliary feedwater
- high pressure safety injection
- low pressure safety injection (residual heat removal)/containment spray injection
- high pressure coolant injection/reactor core isolation cooling
- low pressure coolant injection (residual heat removal)
- SWS (safety system)
- CCWS

Component Boundaries (G1)

No control circuit is included. The main component of a check valve is the valve itself. For the purposes of this study, the boundaries will encompass the valve body including valve internals (e.g. disk, spring) and in the cases of air assisted check valves, valve operators.

Event Boundary

Failure of the CKV to perform its mission occurs if a valve that is required to be open to allow injection or cooling flow does not open, or if a valve that is required to close to isolate secondary parts of the system fails to close.

Basic unit for ICDE event collection

The basic set for check valve data collection is the "exposed population" (EP: set of components exposed to the same failure mechanism). The number of check valves in an exposed population depends on the specific failure identified in the event analysis.

In general the exposed population should be in the same system for the components identified but could be modified depending on the linkage of CCF events by failure mechanism or causal factors.

The exposed population will normally have a similar test interval. Similar in this context means within a factor of 2.

The determination of the exposed population is left to the event reviewer and the reviewer’s knowledge of the relation of system design, operation and testing.

Time frame for ICDE event exchange

The minimum period of exchange should cover 5 years.

Coding Rules and Exceptions

1. All actual failures will be included (in either CCF or independent event coding), even if the event report considers them to be "invalid."

2. Many reports discuss only one actual failure, but state that the other CKV would be susceptible to the same type failure. If there is a statement that the second CKV would have definitely failed, a failure is counted and a CCF is coded. If there is no evidence that the second CKV would have failed due to the same cause, but only that there is a possibility, no CCF is coded.

3. Some reports discuss only one actual failure, and do not consider that the same cause will affect other CKVs, but the licensee replaces the failed component on all CKVs as a precautionary measure. This type of event will be coded as a CCF, with a low (0.1) component degradation value for the components that did not actually fail.

4. In-operability due to seismic criteria violations will not be included, unless an actual failure has occurred.

5. Administrative in-operability that does not cause the valve to fail to function was not included as failures. An example is a surveillance test not performed within the required time frame.

Functional Fault Modes (C03)

Check valve malfunctions are considered to be failures to open or close on demand, and failure to stay closed, including excessive leakage through the valve. Examples of the consequences of these failures are vapour binding AFW pumps, overpressurization of pump suction piping, and system drainage. Failure modes used to analyse check valve data are:

1. Failure to Open (FO)

   Examples are:
   - Check valve sticks closed,
   - Check valve partially opens.

2. Failure to Close (FC)

   Examples are:
   - Check valve sticks open,
   - Valve doesn't fully close, and
   - Failure to re-seat.

3. Failure to Remain Closed/Internal leakage (RC/IL)

   - Cases where the check valve has been closed for a substantial period of time and is then discovered leaking.

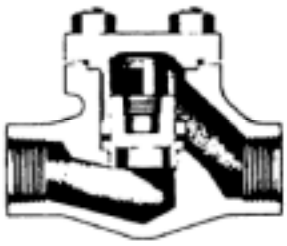
4. External Leaking (EL)

5. Spurious actuation (SA)

Enclosure: Different Check Valves

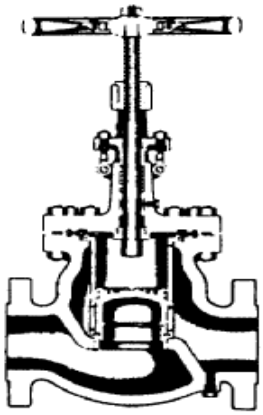
Conventional Swing Check Valve

Clearway Swing Check Valve

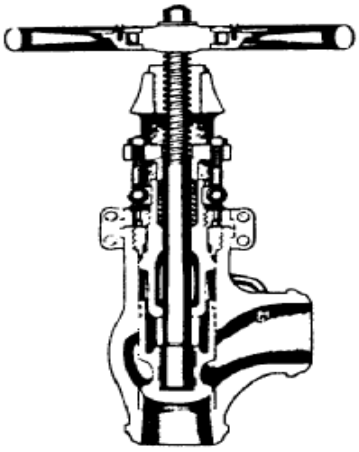


Globe Type Lift Check Valve

Tilting Disc Check Valve



Globe Stop-Check Valve



Angle Stop-Check Valve

ICDE

International Common-Cause-Failure Data Exchange **ICDECG06**

Title: Coding Guidelines for Batteries

Author(s): Marina Concepcion, Wolfgang Werner, Gunnar Johanson, Begoña Pereira Pagan, Jorge Tirira, Ian Morris, Rosa Morales, Anna Oxberry

Issued By: Gunnar Johanson

Reviewed By: Albert Kreuser

Approved By:

Abstract: This report defines the component specific coding rules for Batteries

Doc.ref: Coding Guidelines

Distribution WG, Project Web Site, Project archive

Revision control:

Version	Date	Initial
Draft 1.1	1999-03-18, Initial draft	GJ, MC
Draft 1.2	1999-05-29, Corrected subsystems after Scandinavian WG meeting	MC
Draft 1.3	1999-10-01, Updated subsystems, failure modes, the picture from T-book was removed.	MC
Draft 1.4	1999-12-10, Component boundary picture, updated failure modes, coding rules and exceptions	WW, MC
Draft 1.5	2000-06-21 General description: UPS 2 added and Coding Rules and Exceptions: item 4 corrected	GJ
Draft 1.6	2000-08-21 Inclusion of comments from Rosa and Jorge. 1. General Description of the Component 2. Coding Rules and Exceptions 3. Functional Failure Modes	GJ
Draft 1.7	2000-10-16 Failures of breakers to open added to component boundary and its relation to switchgear/breakers exercise. Enclosure 1 added	GJ
Draft 1.8	2001-04 -12 General Description of the Component; Distinction between DCS 1 and 2 added Coding Rules and Exceptions; clarification to interpretation of degraded and incipient added (item 3)	GJ
Draft 2	2001-05-18 List of authors corrected, Final Draft	GJ
Draft2.1	2001-09-18 Figure 1 is updated several changes in appendix 1	WW, BP
Draft 3	2002-09-10 Addition of item 8 to “Coding Rules and Exceptions” after Paris meeting 04/02	AO

CODING GUIDELINES FOR BATTERIES

General Description of the Component

The family of batteries is comprised of those batteries that provide DC emergency power in the event of a LOSP to DC buses that supply the safety systems of the reactor plant. The voltage to be supplied typically ranges from 24 to 500 V DC.

Battery data are collected for the systems/subsystems

DC power system (3.EE in IRS coding system), consisting of the subsystems
- DCS - DC System. Uninterrupted power supply for emergency DC system and secondary emergency DC system
- DCS-1 - DC System. Uninterrupted power supply for emergency DC system
- DCS-2 - DC System. Uninterrupted power supply for secondary emergency DC system
- IAS-1- Indication and alarm system
- IAS-2- Indication and alarm system of the fire protection
- IAS-3- Indication and alarm system of the control rod drive system
- TCS- Trip circuit supply

For data evaluation purposes, the family of batteries is subdivided into the four subgroups

- BVL - Very low voltage (V= 24)
- BL - Low- voltage battery (24< V< 50)
- BH - High- voltage battery (V>200)
- BM - Medium- voltage battery (50<V<200)

Component Boundaries

The component for this study is the battery, comprised of cell, casing, power leads and their respective output breakers and fuses. The component boundary is illustrated by figure 1.

Included within the Battery is the output breaker (failure to close or remain closed), which is located at the local control. In some cases batteries[1] may have a particular automatic system

Event Boundary

The mission for a battery is to provide DC emergency power in the event of a LOSP to DC buses that supply the safety systems of the reactor plant. Failure of the battery to perform its mission occurs if a battery that is required to supply rated voltage to the DC bus bar fails to do so.

[1] For French plants, 48 V batteries, installed this following an incident at Bugey NNP. This system is part of the 48 V batteries for all NNP in France.

Basic unit for ICDE event collection

The basic set for Battery data collection is the "common-cause component group", (CCCG: set of identical components in a system, performing the same function)

Time frame for ICDE event exchange

The minimum period of exchange should cover 5 years.

Coding Rules and Exceptions

1. In general, the definition of the ICDE event given in section 2 of the General ICDE Coding Guidelines applies.
2. Complete Failure is when power is not maintained within specification
3. Degraded: If cells within the Batteries show major physical, electrical or chemical damage but the batteries are still able to perform within specification OR (Incipient) when slight damage is evident. If there is "no damage" proposed coding should be "working"
4. Some reports discuss only one actual failure, and do not consider that the same cause will affect other BTs, but the licensee replaces the failed component on all BTs as a precautionary measure. This type of event will be coded as incipient impairment (0.1) of the components that did not actually fail.
5. Inoperability due to seismic or electrical separation criteria violations will not be included, unless an actual failure has occurred.
6. Inoperability due to administrative actions that does not cause the battery to fail to function is not included as failures. An example is a surveillance test not performed within the required time frame**.**
7. Guidance for CCF event interpretation (Field C7) and failure mechanism see enclosure 1
8. Consideration of CCF of a single design of battery may be limited to a single location or may extend to different physical locations (e.g. different voltage battery rooms).

Functional Failure Modes

The following failure modes and criticality classifications are applicable for battery data collection.

1. Failure to run (Loss of performance): failure to maintain the rated DC power within specification for the duration of the mission

2. Failure to start (No voltage): the power provided at the start of the mission is not within specification. Could be open circuit, high resistance, or discharged battery i.e. the rated DC power can not be delivered at the time of the demand.

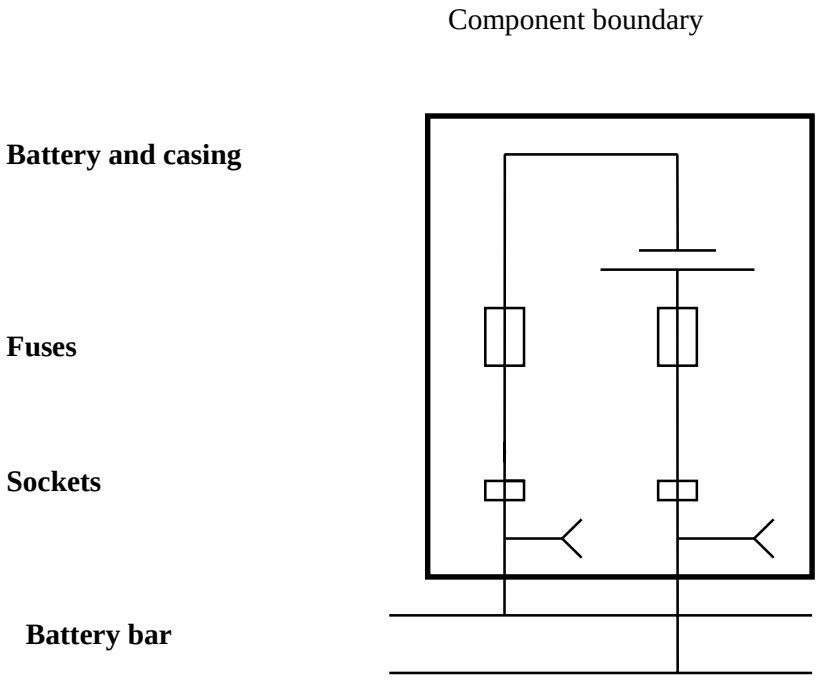


Figure 1. Battery components and boundary

Enclosure

A1. CCF event interpretation (Field C7) and failure symptoms

The CCF event description (Text description /Compulsory/) shall describe the (subjective) rationale used by the analyst to classify the event as a CCF event.

This is a proposal for description of the Failure Symptoms

Code	Failure symptom
BF	Blown fuse
BP	Breaker problem
CB	Casing break
CTP	Corrosion of the terminal plates/insufficient tightening of terminal connections
ICD	**INSUFFICIENT CAPACITY (BY DESIGN)**
IE	Impurities in the electrolyte
LDE	Low density of the electrolyte
LLE	Low level of the electrolyte
OL	**OVERLOADING / EXCESSIVE LOAD**
PDA	Plate degradation (by aging)
RCC	Inadequate room cooling/ventilation conditions
SC	Short-circuit

Remarks:

CB Casing break

Results in electrolyte loss.

CTP Corrosion of the terminal plates / insufficient tightening of terminal connections (improper maintenance)

Results in high electrical resistance due to poor contact between the current conductors; the process leads to a high voltage drop.

ICD Insufficient capacity (by design)

The battery design capacity is inadequate for the system. The battery is working properly, but its capacity is inadequate for supporting loads (i.e. due to design modifications that increased battery loads, or because the initial capacity is insufficient and the problem was only detected in a loss of offsite power incident).

IE Impurities in the electrolyte

The most frequent cause is the use or addition of improper water. (i.e. for Pb batteries, the most common impurities are iron, chlorine, and copper. ***For Ni-Cd batteries, under special battery service conditions, such as high temperature or frequent cycling,the electrolyte absorbs carbon dioxide from the air and it is partially transformed in potassium carbonate,*** increasing the electric resistance and decreasing its capacity; in this situation it could be necessary to replace the electrolyte).

LDE Low density of the electrolyte

Results in progressive loss of the active plate area with the consequential loss of capacity, deformation and deterioration. The problem is detected by the low density of the battery electrolyte. If the sulfurisation is not significant, the battery could be recovered by one or more equalization loads until the proper value of the electrolyte density in all the elements is retained. (Pb-batteries).

LLE Low level of the electrolyte

Results in progressive loss of the active area of the uncovered plate part and the same type of problems as described for the „insufficient load“ case.

OL Overloading / excessive load

This case is characterized by loss of the active material from the plates and the corrosion of the metallic structure in the positive plates. A clear indication of the battery overloading is excessive water use and, therefore, the frequent need to refill the elements in order to maintain the electrolyte level.

PDA Plate degradation (by aging)

The battery is aged, involving capacity loss of the plate. (For Ni-Cd batteries, the aging could be due to the graphite loss: increasing the resistance, causing low voltage and a lower autonomy).

RCC Inadequate Room Cooling/Ventilation Conditions

Room Temperatures:

- too low (for Pb batteries) or too high (for alkaline batteries)
- insufficient ventilation (leading to hydrogen generation).

SC Short-circuit

When two or more plates are in touch, a sudden discharge occurs with subsequent plate destruction.

The most frequent reasons for a short-circuit are:

- accidental introduction of electrically conducting particles into the element, simultaneously contacting two plates of different polarity
- separator wear
- excessive accumulation of sediment at the bottom of the casing (i.e. for Ni-Cd elements, the process is caused by plate carbonating).

This symptom also includes the short-circuit of the power leads from the battery to the bus.

A2. Proposal for the Sub-components and subsystems

CODE	**Sub-component**
BR	Breaker
CE	Cell (elements)
FU	Fuse
PL	Power lead
Other	Other

Notes:

- The battery cells include the connections between cells and the casing.
- The power leads are the external connections from the batteries to the cabinet buses.