Nuclear Safety
NEA/CSNI/R(2011)12
February 2012
www.oecd-nea.org

International Common Cause Failure Data Exchange (ICDE)

General Coding Guidelines
Updated Version
October 2011

NUCLEAR ENERGY AGENCY

Unclassified **NEA/CSNI/R(2011)12**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **21-Feb-2012**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Cancels & replaces the same document of 15 February 2012

INTERNATIONAL COMMON CAUSE FAILURE DATA EXCHANGE (ICDE)

General Coding Guidelines - Updated Version

October 2011

This report is an update of the report NEA/CSNI/R(2004)4 with new developments achieved by the ICDE Project.

JT03316398

NEA/CSNI/R(2011)12
Unclassified

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 34 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, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, 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 30 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission 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 the 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 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 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 Committee on Radiation Protection and Public Health and NEA 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 boulevard des Iles
92130 Issy-les-Moulineaux
France

REVISION CONTROL

Title:	CSNI Tech Note publication NEA/CSNI/R(2004)4 International Common Cause failure data Exchange ICDE General Coding Guidelines Technical Note: October 2011 Initially issued as CSNI Report: Tech Note Publication NEA/CSNI/R(2004)4		
Revision control:	Version		Initial
2003-10-27	Final	ICDECG00 Revision 8.1 – Final Edition for CSNI Tech Note publication	
January 2004		Issued as NEA/CSNI/R(2004)4	NEA
	Internal ICDE		
2004-12-28	Revision 1	Corrections following ICDE SG meeting 20 S5 – Added description of calculator C11 – Added missing compulsory requirement C14 – Added footnote. Changed in related text to "occurred".	GJ
2005-10-26	Revision 2	Corrections following ICDE SG meeting 21 C14 – Changes as stated in 21st SG protocol	GJ
2006-08-30	Revision 3	Corrections following ICDE SG meeting 23, action item 23-16. CCCGs renamed as observed population. New internal version with appended LM, breaker and CRDA component coding guidelines	WW/GJ
2007-08-30	Revision 4	Added complete CCF event definition in Chapter 2 Section 10	GJ
2007-12-27	Revision 5	The component guides has been augmented by the associated IRS codes	WW/GJ
2009-03-25	Revision 6	Corrections according to "Comment IRS codes ww ak ao rev1" p38, 44, 57, 69, 70, 71, 72.	GJ
2009-09-17	Revision 7	Revisions according SG 29 Actions 29-7 latent time and 29-10 essential failure modes	WW
2010-08-23	Revision 8	Revisions according SG 31(-9) and work notes on Actions 30-1, 30-16 and 30-17	GJ
2011-10-18			

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).
Dr. Albert Kreuser (GRS).

In addition, those persons who have contributed to the component specific guidelines are mentioned in the respective appendices ICDE CG 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.
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 so called "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. **"**Partial CCF" is also of interest and is defined as complete failure of at least two components, but not all of the exposed population, where these fault states exist simultaneously and are the direct result of a shared cause.

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

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)AND EXPOSED POPULATION (EP)

An **Observed Population (OP)** is 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.

Frequently, an OP is a collection of all similar components within one system (e.g. all MOV in the Auxiliary Feed Water System or all motor-driven pumps in the Residual Heat Removal System), but there may be cases in which OPs contain components of more than one system (if components of same design in further systems operate under equal conditions). Also, the components of the OP may perform different functions, for example, an OP may contain suction and discharge valves. Often, the OPs are the redundant, identical components of a system, all performing the same function and thus are equal to the common cause component groups (CCCGs) explicitly modelled in many probabilistic safety analyses. Example: parallel pumps in a multi-train injection system.

OP records (also called group records) as defined in chapter 4 include technical and statistical information to allow for data collection needs and for CCF-quantification needs for all types of components. For some quantification models not all the information about the components in the OP records is necessary, such as number of demands or the time period indicating the observation time and independent failure counts.

A subset of the Observed Population is the **Exposed Population (EP)**. EP is a data collection concept used for reporting events. Its composition is defined by the reported event.

In an actually observed CCF event some or all components of an EP are exposed to a common causal mechanism, but may be affected differently: some may fail completely, some may be degraded, while others remain unaffected. The suffered impairment is described by the component impairment vector (the length of which is equal to the number of components exposed to the event). The impairment attribute "working" is assigned to those exposed components that did not suffer impairment from the CCF event.

For each component type included in ICDE, a component-specific coding guideline is developed, defining the component boundaries, event boundary, coding rules and exemptions, and functional fault modes.

We note that the number of components in an EP is less than or equal to the number of components in the corresponding OP. Similarly, the number of component in a CCCG is less than or equal to the number of components in the OP. The size of an EP and CCCG can differ; they may be equal, one can be less than the other.

4. OBSERVED POPULATION 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 Identifier

Code/Automatic

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

G1 Observed Population 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. If no further subdivision is reasonable 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, 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 Populations are the basic sets of components in the context of CCF data base set-up and analysis. The size of the Observed Population is the number of similar/redundant components in the system that are potentially susceptible to the same failure mechanism. The Observed Population is assumed to be internally homogenous, differences should be described. In some exceptional cases 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 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

Numeric (Compulsory in G1)

The Size of the Observed Population is the number of components put together in the Observed Population defined in G1.

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 identifier" to distinguish otherwise identical "G0 identifiers".

5. STATISTICAL RECORD FOR THE OBSERVED POPULATION

S1 Component failure modes

Code/Compulsory

The components of the Observed Population 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 component 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

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

Numeric/Compulsory

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

S3 Start of observation time for Observed Population

Date/Compulsory

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

Format: YYYY/MM/DD

S4 End of observation time for Observed Population

Date/Compulsory

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

Format: YYYY/MM/DD.

The total Observed Population 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 Observed Population, 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.

If the flag "Real count" is set only complete failures are to be included among the independent failures.

If the flag "Estimated" is set, then the generic failure rate (per hour) and/or generic failure probability per demand are indicated in a "calculation note" field including an uncertainty measure like the ratio between the 95% and 50% quartile of the failure rate distribution and information on how the value for the Number of independent failures in S5 has been generated.

Standby failures modes

Assuming standby failures, a calculator can make a proposal for the value in field S5 using the following formula:

Model 1 Standby failures:
S5 = (Generic failure rate per hour) × (G6 Size of Observed Population) × (S2) × (Observed Population observation time (S4-S3)) × (24 hours per day)
+
(Generic failure probability per demand) × (G6 Size of Observed Population) × (S2) × ((Observed Population observation time (S4-S3)) / (G5-1 Test interval)) or S7 Demand cycles)

Note: The calculator will need input of the standby failure rate or failure probability on demand or both. If failure probability is used the calculator can guess the number of demand cycles using the observation period and test interval or use the optional S7 input if available.

Operational failures modes

Assuming operational failures, the calculator can make a proposal for the value in field S5 using the following formulas:

Model 2 Operational failures (operational components):
S5 = (Generic failure rate per hour) × (G6 Size of Observed Population) × (S2) × ((Observed Population observation time (S4-S3) or S6 exposure time)

Model 3 Operational failures (standby components):
S5 = (Generic failure rate per hour) × (G6 Size of Observed Population) × (S2) × (((Observed Population observation time (S4-S3)) / (G5-1 Test interval)) or S7) × (Average mission time)

Note: The calculator will need input of the operational failure rate. If model 2 is used the calculator can guess the exposure time using the observation period or use the optional S6 input if available. If model 3 is used the calculator will need input of an average mission time (the average running time at test). The calculator can guess the number of demand cycles using the observation period and test interval or use the optional S7 input if available.

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.
- 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 identifier

Code/Automatic

See Observed Population 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 /except for "latent time", which is optional

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 (optional), 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 many cases, this number will be the same as the Observed Population size. However, as specific failure events may not affect all components of an Observed Population the appropriate number can also be smaller than the Observed Population size (see definition in section 3).

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, e.g.:

- 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, e.g.:

- 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 OP 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/Compulsory

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:

High

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".

Note: ?

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 or the time between occurrences 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 occurred or were 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 occurred or were 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 occurred or were discovered[*] during testing or by observation two test cycles apart (at time 2T). The weight factor is 0.1.

[*] If occurrence time cannot be estimated.

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.
- Flow strainers used "temporarily" during plant commissioning were found in several pipelines in consecutive refueling outages (1 year apart). The time factor is "high" because failures (errors) occurred close in time (at commissioning), even if they were discovered far apart.

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 01-09

ICDE

International Common-Cause-Failure Data Exchange **ICDE CG 01**

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		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
2009-09-11		Update in the part Functional fault modes	WW

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 (the corresponding IRS system coding is added in parentheses):

- Auxiliary/emergency feedwater (3.BB).
- High pressure safety injection, (PWR (3.BG)).
- Low pressure safety injection, (may include residual heat removal) PWR (3.BG).
- Gas circulators GCR (3.BG).
- Residual heat removal (if out of emergency core cooling function), PWR and BWR (3.BE).
- Containment spray (3.DD).
- Ice condenser (3.DD).
- High-pressure coolant injection/reactor core isolation cooling, (BWR) (3.BA).
- Low-pressure coolant injection, (may include residual heat removal) BWR (3.BG).
- Component cooling, including reactor building closed cooling water (3.CA).
- Pressure vessel cooling and reactor ancillaries cooling GCR (3.CA).
- Essential SWS (3.CB).
- Essential raw cooling water (3.CB).
- Standby liquid control, (BWR) (3.BD).
- LP and HP main and standby boiler circulating water pumps GCR (3.DG).
- Emergency power generation and auxiliaries, including supply of fuel and lubrication oil (3.EF).

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 the observed population (OP). The OP 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 January 1st, 1990 – December 31st, 1994, ref. Park City protocol).

Coding Rules and Exceptions

In general, the definition of the ICDE event given in section 2 of the General ICDE Coding Guidelines applies.

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

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.

Failure of the electrical operator without coincident failure of the manual operator is considered a CP failure.

In-operability due to human error or erroneous calibration/set up will be included (in either ICDE or independent event coding).

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

Essential failure 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).

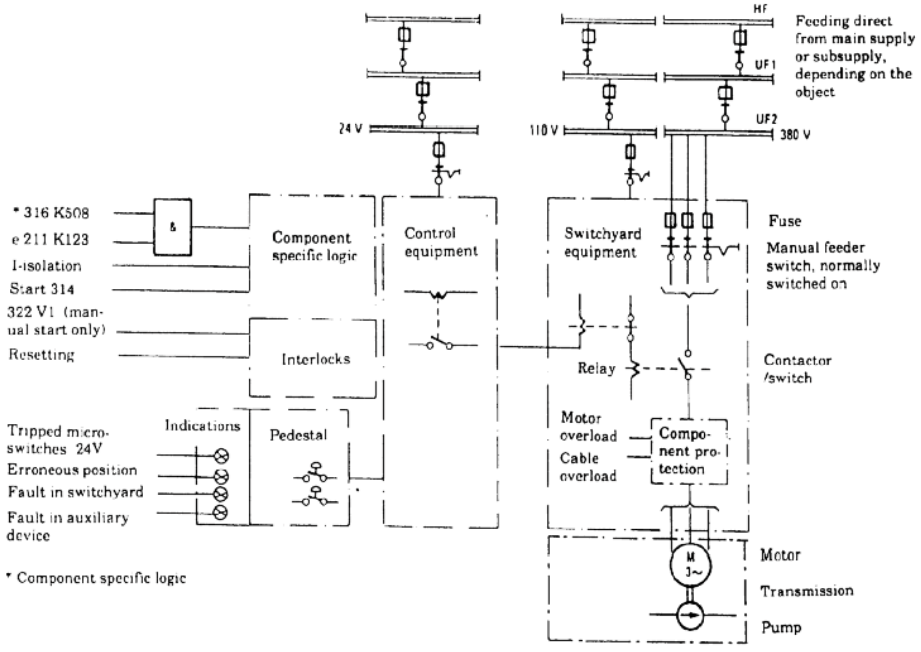
Several countries also have:

3. Failure to stop/close (FC).
4. 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 **ICDE CG 02**

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		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
Jan 2004		Issued as NEA/CSNI/R(2004)4	GJ
2009-09-11		Update in the part Functional fault modes	WW

Component 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 (the corresponding IRS system coding is added in parentheses):

- Auxiliary/emergency feedwater (3.BB).
- High pressure safety injection (3.BG).
- Low pressure safety injection (may include residual heat removal), PWR (3.BG).
- Residual heat removal (if out of emergency core cooling function), PWR and BWR (3.BE).
- Refuelling water storage tank (3.CD).
- Containment spray (3.DD).
- Pressurizer power operated relief valve block valves (3.AF).
- High pressure coolant injection/reactor core isolation cooling , (BWR) (3.BA).
- Low pressure coolant injection (may include residual heat removal), BWR (3.BG).
- Isolation condenser, (BWR) (3.DD).
- Component cooling water (3.CA).
- Essential SWS (3.CB).

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 "observed population" but if appropriate the exposed population is taken (EP: set of components exposed to the same failure cause). 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 January 1st, 1990 - December 31st, 1994, ref. Park City protocol).

Coding Rules and Exceptions

In general, the definition of the ICDE event given in Section 2 of the General ICDE Coding Guidelines applies.

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.

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

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.

Failure of the electrical operator **without coincident failure of the manual operator** is considered a MOV failure.

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

Essential failure modes:

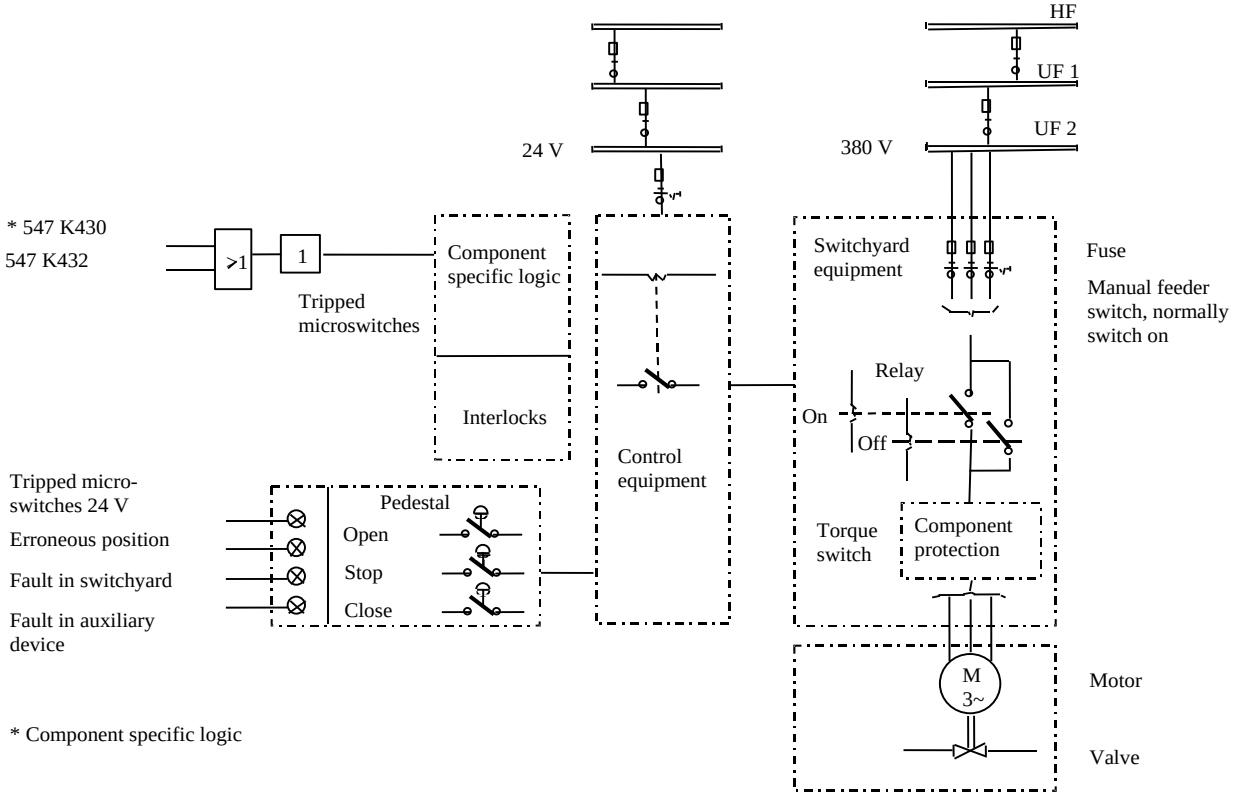
- Failure to open (FO)
- Failure to close (FC)
  (for some valves only 1 of the 2 failure modes is relevant)

Several countries also have:

- Internal Leakage (IL)
- External Leakage (EL)

Component boundaries (next page)

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



ICDE

International Common-Cause-Failure Data Exchange **ICDE CG 03**

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		Initial
1999-01-13	Draft 2	Final Draft	GJ
Jan 2004		Issued as NEA/CSNI/R(2004)4	

Component 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.

The systems for which emergency diesel generator (EDG) data are collected are (the corresponding IRS system coding is added in parentheses):

- Auxiliary/emergency feedwater (3.BB).
- High pressure and low pressure safety injection, (3.BG).
- Emergency power generation and auxiliaries, including supply of fuel and lubrication oil (3.EF).

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 observed population (OP). The OP size typically varies from two to eight, with the bulk ion the 2 to 4 range.

Time frame for ICDE event exchange

The minimum period of exchange should cover a period of 5 years (The initial pump exchange cover January 1st, 1990 – December 31st, 1994, ref. Park City protocol).

Coding Rules and Exceptions

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.

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.

In general, the definition of the ICDE event given in Section 2 of the General ICDE Coding Guidelines applies.

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.

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)

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

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.)

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

Essential failure modes:

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.

Failure to run (FR.). The /EDEDG must be loaded (required for the current conditions) and stable prior to the failure.

Several countries also have:

Failure to stop (FC).

ICDE

International Common-Cause-Failure Data Exchange **ICDE CG 04**

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		Initial
1999-05-10,	Draft 1.5	Corrections following the Paris meeting Revised component classification.	GJ
2000-05-01,	Draft 1.6	Clarification failure mode example	GJ
2000-10-06,	Draft 1.7	Update of component types so that they can be used for Magnox and AGR.	EJ
2002-10-02	Draft 1.8	Editorial	GJ
January 2004		Issued as NEA/CSNI/R(2004)4	
2010-08-23		Update in the part Functional fault modes	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 (the corresponding IRS system coding is added in parentheses):

- Steam generators discharge headers, PWR, AGR, Magnox (3.AH)
- Pressurizer vapour volume, PWR (3.AF)
- Reactor coolant system, main steam headers, BWR, AGR, Magnox (3.BH)

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 observed population (OP). The OP 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 Fault 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:

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

Failure to Close (FC): Examples are: SV/RV stays open when it should close, SV/RV does not fully close.

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 (for some valves only 1 or 2 of the 3 failure modes are relevant).

Several countries also have:

- Internal leakage (IL)

- Spurious operation (SO). This code may be used e.g. for failure to stay open.
- Others (O)

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.

<u>Enclosure:</u> Component picture of safety/relief valves

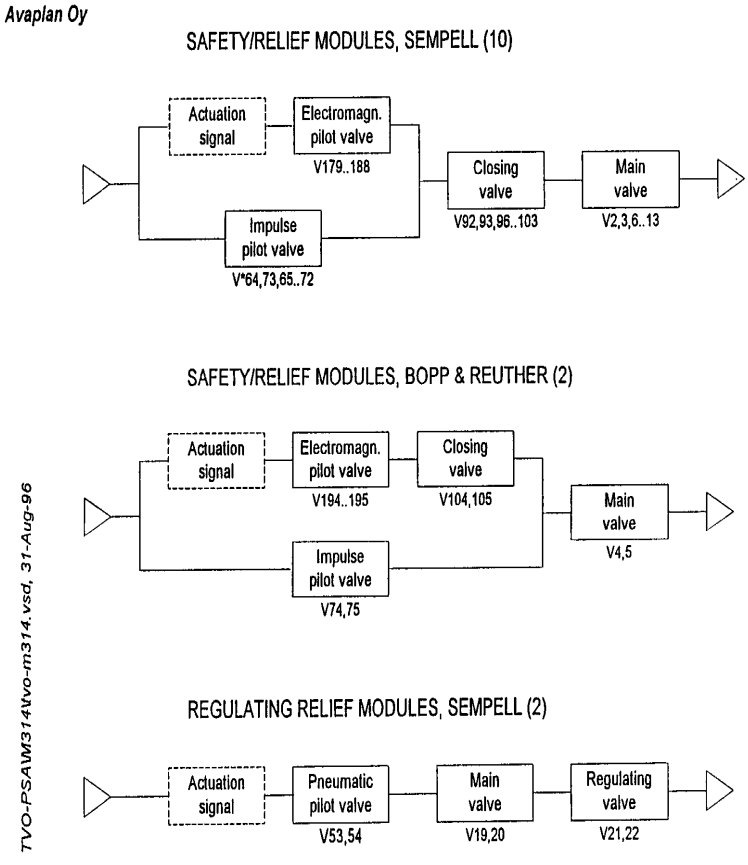


Figure 1.1

CC-SRVup, 4( )

ICDE

International Common-Cause-Failure Data Exchange **ICDE CG 05**

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		Initial
	Draft 1.2	Components types; failure modes	MC
1999-05-03,	Draft 1.3	Corrections following the Paris meeting	GJ
1999-07-08	Draft 1.4	Component types details	MC
2000-05-15	Draft 1.5	Clarifications, rules and exemptions	GJ
2000-10-18	Draft 1.6	Enclosure – Figures are included	EJ
Jan 2004		Issued as NEA/CSNI/R(2004)4	
2009-09-11		Update in the part Functional fault modes	WW

Component Coding Guidelines for Check Valves

General Description of the Component

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.
- Pump turbine steam inlet.

The following component classification is proposed:

- Swing check valve.
- Lift check valve.
- General type.

The following details about component can be included in general description.

- 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

The systems for which check valve (CKV) data are collected are (the corresponding IRS system coding is added in parentheses):

- Auxiliary/emergency feedwater (3.BB).
- High pressure safety injection (3.BG).
- Low pressure safety injection (may include residual heat removal), PWR (3.BG).
- Residual heat removal (if out of emergency core cooling function), PWR and BWR (3.BE).
- High pressure coolant injection/reactor core isolation cooling, BWR (3.BA).
- Low pressure coolant injection (may include residual heat removal), BWR (3.BG).
- Component cooling, including reactor building closed cooling water (3.CA).
- Essential SWS (3.CB).

Component Boundaries

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 "observed population" but if appropriate the exposed population is taken (EP: set of components exposed to the same failure cause). 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

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

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.

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.

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

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.

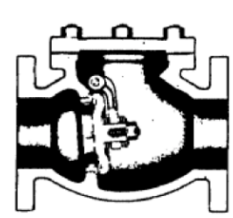
Functional Fault Modes

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:

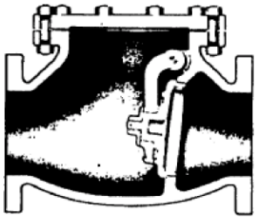
- Essential failure modes:
  - ↳ Failure to Open (FO)
    Examples are:
    - Check valve sticks closed,
    - Check valve partially opens.
  - ↳ Failure to Close (FC)
    Examples are:
    - Check valve sticks open,
    - Valve does not fully close, and
    - Failure to re-seat.

  (for some valves only 1 of the 2 failure modes is relevant)
- Several countries also have:
  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.
  - External Leakage (EL)
  - Other (O)

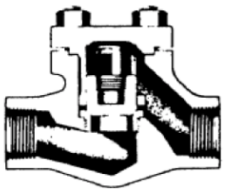
Enclosure: Different Check Valves



Conventional Swing Check Valve

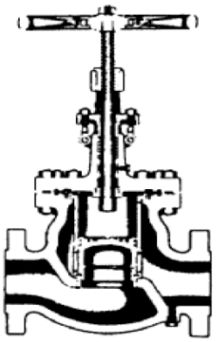


Clearway Swing Check Valve

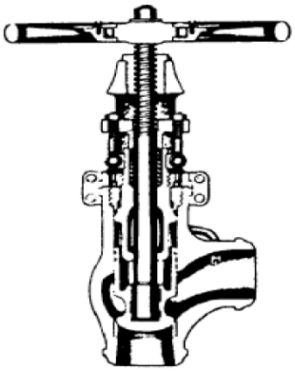


Globe Type Lift Check Valve

Tilting Disc Check Valve



Globe Stop-Check Valve



Angle Stop-Check Valve

ICDE

International Common-Cause-Failure Data Exchange **ICDE CG 06**

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
2001-05-18	Draft 2	List of authors corrected, Final Draft	GJ
2001-09-18	Draft2.1	Figure 1 is updated several changes in appendix 1	WW, BP
2002-09-10	Draft 3	Addition of item 8 to "Coding Rules and Exceptions" after Paris meeting 04/02	AO
January 2004		Issued as NEA/CSNI/R(2004)4	
2009-09-11		Update in the part Functional fault modes	WW

Component 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 (the corresponding IRS system coding is added in parentheses):

Vital instrumentation AC and control AC (3.ED)

DC power system (3.EE), 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 batteries1 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.

Basic unit for ICDE event collection

The basic set for Battery data collection is the observed population (OP).

Time frame for ICDE event exchange

The minimum period of exchange should cover 5 years.

Coding Rules and Exceptions

In general, the definition of the ICDE event given in Section 2 of the General ICDE Coding Guidelines applies.

Complete Failure is when power is not maintained within specification

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"

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.

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

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.

Guidance for CCF event interpretation (Field C7) and failure mechanism see enclosure 1

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).

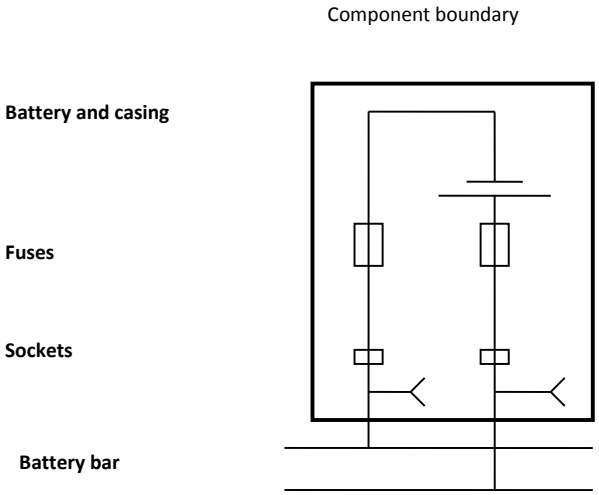
Functional Fault Modes

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

- Essential failure modes:
  - Failure to run (Loss of performance): failure to maintain the rated DC power within specification for the duration of the mission
  - 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 cannot be delivered at the time of the demand.

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.

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.

ICDE

International Common-Cause-Failure Data Exchange ICDE CG 07

Title:	Coding Guidelines for Level Measurement		
Author(s):	Albert Kreuser		
Issued by:	Albert Kreuser		
Reviewed by:	WG		
Approved by:			
Abstract:	This report defines the component specific coding rules for Level Measurement.		
Doc. Ref:	Coding Guidelines		
Distribution:	WG, Project Web Site, Project archive		
Revision control:	Version	Date	Initial
	Final	2006-01-31	AK
2009-09-11		Update in the part Functional fault modes	WW

Component Coding Guidelines for Level Measurement

General Description of the Component

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

The vessels, tanks and piping (denoted as "vessels" in the following) at which *Level Measurement* is installed and data are collected are (the corresponding IRS system coding used in field G 3.1 and the IRS system names are added in parentheses):

1. Pressurizer (PWR, PHWR), (3.AF – Pressure control (includes primary safety relief valves)).
2. Steam generators secondary side (PWR, PHWR), (3.AH – Steam generator, Boiler, Steam drum).
3. Accumulators (PWR), (3.BL - Core flooding accumulator (PWR with upperhead injection system)).
4. Reactor refuelling water storage tanks (PWR, PHWR), (3.CD – Borated or refuelling water storage (PWR)).
5. Reactor coolant lines (mid-loop operation) (PWR), [3.AE – Primary coolant (pumps and associated materials, loop piping, ...)].
6. Containment sump (PWR, BWR), [3.BG – Emergency core cooling (core spray or RHR, CVCS participation)].
7. Reactor pressure vessel (PWR, BWR), [3.AC – Reactor vessel (with core internals, PHWR or LWGR pressure tubes, ...)].
8. Suppression pool (BWR), [3.BA – Reactor core isolation cooling (BWR)].
9. Reactor scram tanks (BWR), [3.AB – Control rod drive (mechanism, motor, power supply, hydraulic system, other shutdown systems)].
10. Calandria (PHWR), [3.AC – Reactor vessel (with core internals, PHWR or LWGR pressure tubes, ...)].
11. Chemical and Volume Control System (PWR), (3.BF – Chemical and volume control (PWR with main pumps seal water, ...)).

The vessels, numbered 1 through 11 in correspondence with the above list, are to be selected from the pull down menu in field G 3.2. For a chosen vessel the process engineering system of that vessel is chosen from the pull down menu of field G 3.1, for example, if Suppression pool (BWR) (#8) is chosen for vessel from G 3.2, the system 3.BA - Reactor core isolation cooling (BWR) (#8) has to be chosen from G 3.1.

Pressure transmitters/sensors are the central instrument of the component *Level Measurement* The following component types of transmitters/sensors are distinguished:

- Pressure difference transmitter with electric output signal (Barton-cell) (PDTE).
- Pressure difference transmitter of membrane type with electric output signal (PDTM).
- Pressure difference sensor, Bourdon type (PDSB).
- Sensor with ultrasonic measuring cell (SUMC).
- Sensor with capacitance measuring cell (SCMC).
- Pressure difference sensor with piezoelectric transducer (PDSP).
- Sensor with resistance thermometer (SRT).
- Becker core cooling monitoring (voltage drop when measuring temperature in transmitter) (BCCM).
- Level Measurement general (LM) (transmitter/sensor type not specified).

Component Boundaries

The component boundary in this data analysis includes the following: pressure gauge lines, isolation valves, transmitter or sensor, indicating instruments, electronic limit switches. A detailed example of the electric part of *Level Measurement* component is given in the component boundary diagram in the Appendix.

As redundancy degrees of parts of the equipment may differ, e.g. one pair of pressure gauge lines can be connected to several transmitters, four sub-components are defined:

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

A separate observed population record is defined for each sub-component (analogous to SRV database). Observed population record field G1 "Definition" for transmitter (or sensor) sub-component (the central equipment of *Level Measurement*) should describe the relation between the sub-components of the component *Level Measurement* (e.g. which transmitters are connected to one pair of pressure gauge lines etc.) This description is necessary to understand the consequential failures of *Level Measurement* resulting from sub-component failures.

Event Boundary

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

Note: triggering of limit switches of *Level Measurements* in response to an actual high or low level is not a failure.

Basic unit for ICDE event collection

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

Time Frame for ICDE Event Exchange

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

Functional Fault Modes

Level Measurement malfunctions are defined as failures to indicate level during operation and failures to trigger limit switch on demand. The failure modes used in evaluating the data are:

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

- Example for complete failure: Signal rises to full scale deflection although actual level in vessel does not change.
- Example for degraded failure: Signal drifts from actual value for more than some level that does not compromise the safety function.
- Example for incipient failure: Signal drifts from actual value less than this level but more than accuracy of measuring instrument.

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

- Example for complete failure: Signal drops to zero although actual level in vessel does not change
- Example for degraded failure: Signal drifts from actual value for more than some level that does not compromise the safety function.
- Example for incipient failure: Signal drifts from actual value less than this level but more than accuracy of measuring instrument.

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

- Examples for complete failure:
- Signal keeps its value when level in vessel changes.
- Transmitter or limit switch is so severely miscalibrated or drifted that specified limits would not be triggered.
- Example for degraded failure: Drift or set point of limit switch off the required value for more than some level that does not compromise the safety function.
- Example for incipient failure: Drift or set point of limit switch off the required value, not compromising the safety function, but more than adjustment accuracy of equipment.

General instrument failure (if no other failure mode is coded) (GIF)

Several countries also have:

- Unstable signal (spurious activation) (IO).
- Instrument inoperability (II).
- Instrument out of specification (IOS).

General 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. All actual failures will be included (in either ICDE or independent event coding), if they could have occurred during a relevant operating mode or state.
3. Some reports discuss only one actual failure, and do not consider that the same cause will affect other Level Measurements, but the licensee replaces the failed equipment on all Level Measurements as a precautionary measure. This type of event will be coded as a CCF, with a low (0.1) component degradation value for the components that did not actually fail. This also applies if it was decided to implement said replacement at a later time.

4. Administrative in-operability that does not cause the Level Measurement to fail to function is not included as failures. An example is a surveillance test not performed within the required time frame.
5. In-operability due to human error or erroneous calibration/set up will be included (in either ICDE or independent event coding).
6. In-operability due to seismic criteria violations will not be included.

Recommendations on OPs

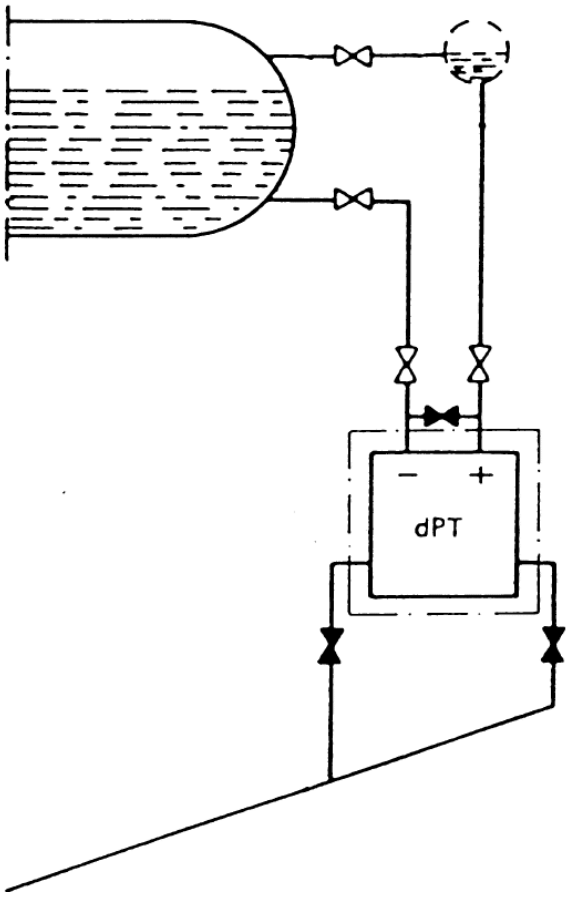
1. Use the subcomponent feature of the database to build OP records with different degrees of redundancy to describe the equipment for one system (i.e. a vessel in the level measurement database).
2. The idea for grouping should be to include all equal equipment in one OP. Examples:
   - ~ All limit switches – even if connected to transmitters of different type
   - ~ Equal equipment for level measurement of several boilers or steam generators in one plant
   - ~ Identical equipment that belongs to two different shut down systems but both systems have the same function of level measurement for one vessel (with the only difference that it is maintained by different maintenance teams) should be in 1 group because there is no significant difference between the components.
   - ~ If there are different numbers of sensors from pairs of gauge lines, define sensors in 1 OP and gauge lines in another.
   - ~ Transmitters of different types/technologies can be put in one OP, but description should justify why.
   - ~ Transmitters from different manufacturers but otherwise same type should be put in one OP. The discriminating feature "manufacturer" can be considered in the PSA model.
3. The degree of detail of the description in the OP definition field G1 is essential to understand both the technology of the equipment and the grouping of the components. The description should explain the reasons for grouping components in one OP. It is important to understand why components belong to one group.
4. If a group of components is described on subcomponent level this should be mentioned in the G1 definition field. Mention also the related subcomponent group records. The relationship between subcomponents should be defined clearly.
5. If more than one OP is set up for one type of subcomponents in one vessel, the description in the G1 definition field should explain the difference between these OPs (e.g. different function in the system).
6. The field G8 (OP Number) can be used to distinguish records if several OPs would have otherwise identical field G0 (OP Name)
7. For very complex systems (e.g. level measurement of the BWR reactor pressure vessel and the BWR reactor scram tanks) a diagram may be needed to understand the relationship of the components. Such diagrams can be added to this coding guide.
8. If equipment was changed during the data collection period (e.g. redundancy, technology of the transmitters) it is reasonable to create two sets of OPs. The definition in G1 benefits from up-front description of changes made.
9. Information about scope of tests is needed to decide about: is time factor high or low for two failures which are separated by time. An explanation should be given in the definition field G1 about the test interval (surveillance test or more thorough test with longer time interval). The coded test interval should be the shortest interval.
10. Abbreviations in descriptions should be explained.

Recommendations on CCF event descriptions

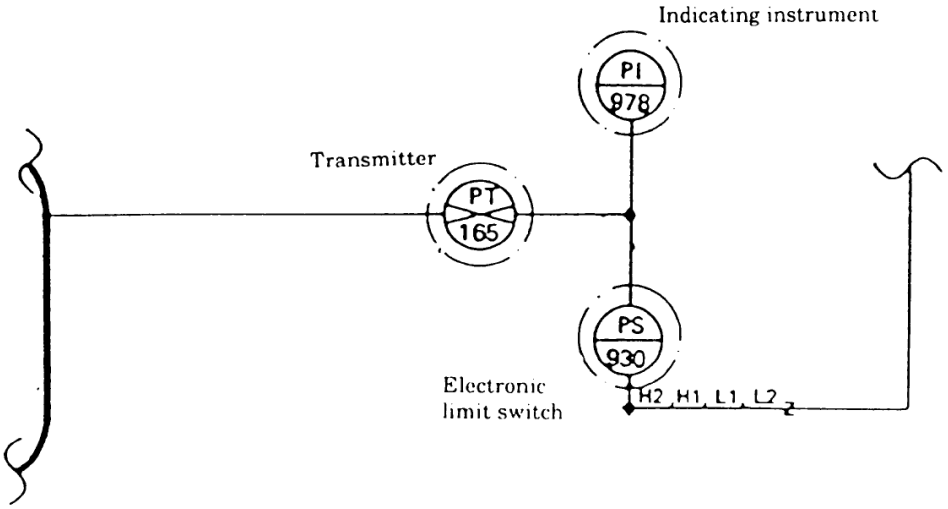
1. If a CCF event affected components that belong to 2 OPs then 2 event records should be made. Each event record should describe the observed impairments of the components of its corresponding OP.
2. In order to be able to validate the impairment coding the event description field C5 should contain information that explains the impairment coding. (E.g. the magnitude of deflection of a transmitter signal should be given if available.)
3. Latent time (field C2-2) is put to 0 for monitored failures only. If components are not permanently monitored but are checked regularly (e.g. on walk downs), latent time is e.g. 1 day. It is possible that an event with latent time 0 has a time factor "High" (e.g. multiple failures to run during mission time). Latent time can be larger than the shortest test interval (which is indicated in field G5-1 of the OP record) if a failure cannot be detected in e.g. 3 monthly routine testing, only in e.g. 3 yearly intensive testing. This should be explained in the event description field C5.
4. It has to be recognized that for some events the information given is all information available from the original records but description may not be clear enough to understand e.g. the detection means or the degree of impairment.
5. Root cause coded in field C9 is a high level classification. The value list of field C9 does not represent "real" root causes. These are only described in the event description field C5.
6. If some but not all components failed in a system containing several vessels (e.g. steam generators) it matters to know whether the failures were on the same or on different vessels. This information may be important to know how to prevent or to protect.
7. If not obvious, additional information is needed to understand number of exposed components.
8. If available, event description should mention the safety consequences of the observed failure to the component, e.g. is the signal deflection to the high or low side
9. If not obvious, event description should clarify reasoning for root cause coding, corrective action coding etc.

Appendix

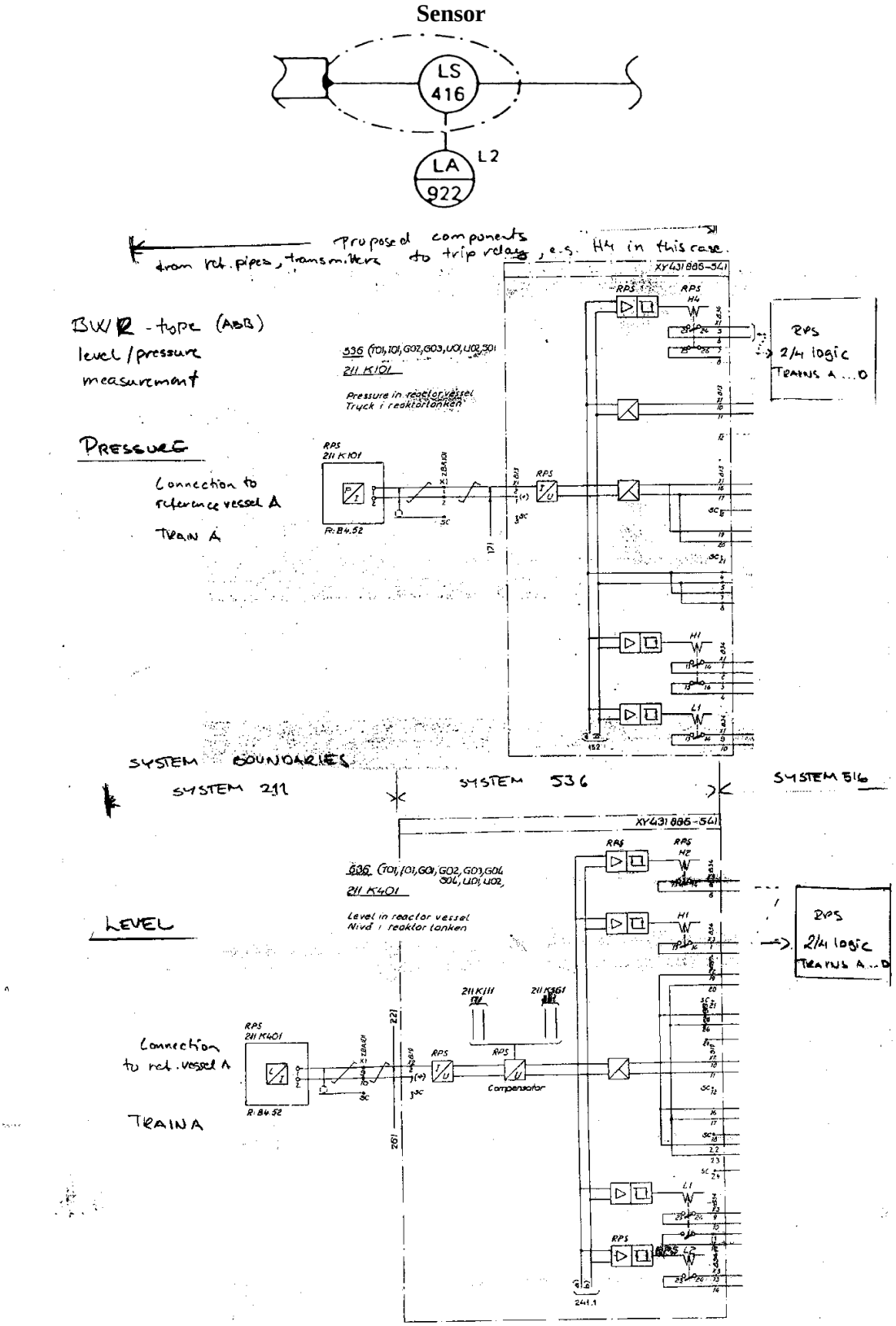
Sub-component boundary for level transmitters (within dotted line) and pressure gauge lines (from T-Book 5th edition, Chapter 11, Figure 9)



Sub-component boundary of transmitters, electronic limit switches and indicating instruments (from T-Book 5th edition, Chapter 11, Figure 5)



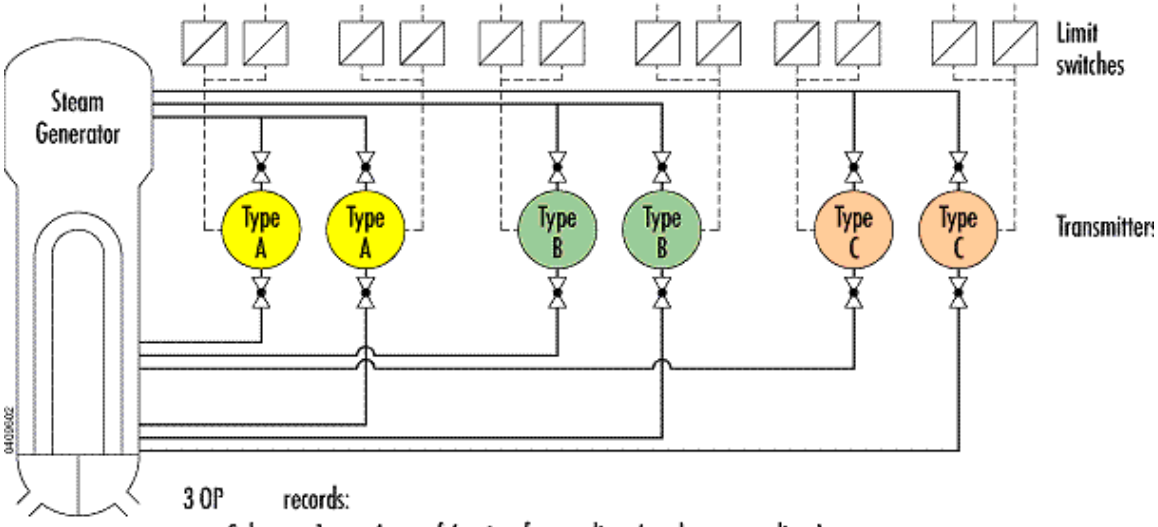
Sub-component boundary of sensors (from T-Book 5th edition, Chapter 11, Figure 5)



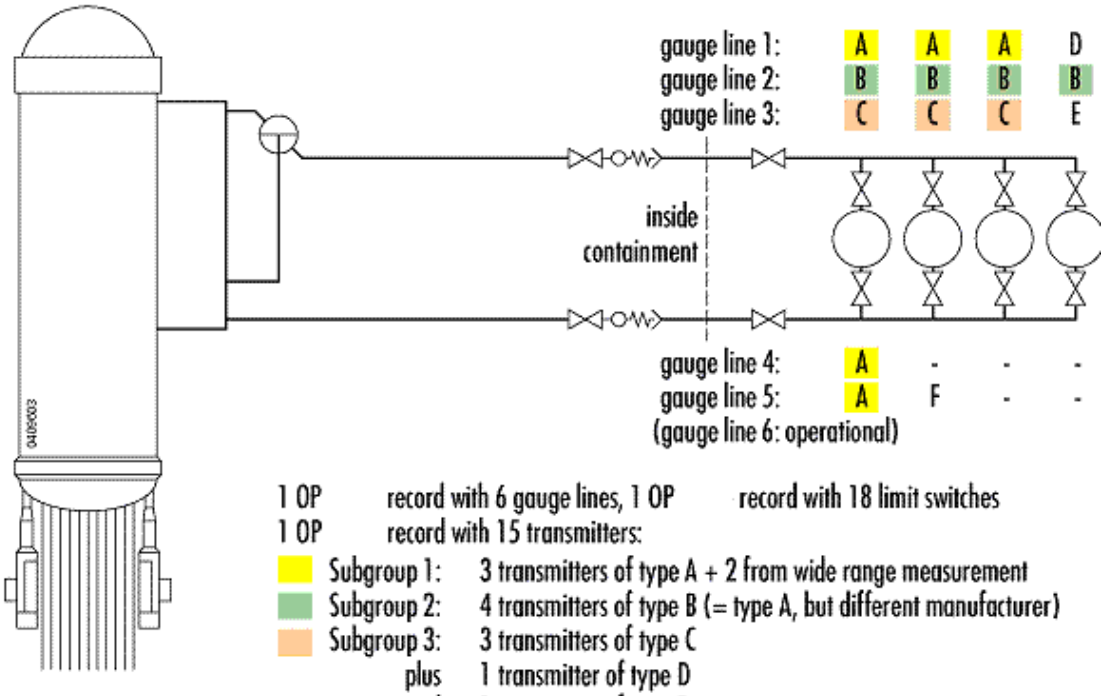
Component boundary for the electric part of Level Measurement component (from TVO BWR plants)

Observed Population examples

ICDE-Level Measurement: OP - 4 Steam Generators



ICDE-Level Measurement OP - BWR: Reactor Pressure Vessel



1 OP record with 6 gauge lines, 1 OP record with 18 limit switches
1 OP record with 15 transmitters:

- Subgroup 1: 3 transmitters of type A + 2 from wide range measurement
- Subgroup 2: 4 transmitters of type B (= type A, but different manufacturer)
- Subgroup 3: 3 transmitters of type C
- plus 1 transmitter of type D
- and 1 transmitter of type E
- and 1 transmitter of type F from wide range measurement

ICDE

International Common-Cause-Failure Data Exchange **ICDE CG 08**

Title:	Coding Guidelines for Switching Devices and Circuit Breakers		
Author(s):	Begoña Pereira; María Rosa Morales; Ian Morris; Fritiof Schwartz; Rafael Cid; Dale Rasmuson; Anna Oxberry		
Issued by:			
Reviewed by:	Wolfgang Werner		
Approved by:			
Abstract:	This report defines the component specific coding rules for Switching Devices and Circuit Breakers		
Doc. Ref:	Coding Guidelines		
Confidentiality control:	Confidential under OECD/NEA agreement		
Distribution	WG, Project Web Site, Project archive		
Revision control:	Version	Date	Initial
	Draft 1.1	2002-04-12, Initial draft 2002-10-22, 2nd draft	BP, RM, IM, FSZ
	Draft 1.2	2002-11-15 Coding rules and exceptions modified, Failure Criteria and Definitions included. 2003-01-27 Reactor Trip Breaker Definition included 2003-03-24 QA comments included. 2003-04-23 First Draft. 2003-06-24 2nd Draft 2003-08-22 2rd Draft (SG comments included). Figure 1-1 changed.	BP, RM, RC, DR, WW, AO, AK, JT
	Draft 1.3	2005-03-17 Air Circuit Breaker definition included in Appendix A.	RM, BP
2009-09-11		Update in the part Functional fault modes	WW

Component Coding Guidelines for Switching Devices and Circuit Breakers

General Description of the Component

The switching devices and circuit breakers of interest are those that belong to (Low/Medium Voltage) Electrical Distribution Systems (busbar/MCC[1] feeder and load breaker) and Reactor Trip Breakers.

Diesel Generator (DG), Motor Operated Valve (MOV), and Motor Pump (MP) breakers are included within their equipment boundaries.

The reactor trip breakers (RTBs)[2] are part of the reactor protection system (RPS), and supply power to the control rod drive mechanisms. Both AC and DC breakers are used for the RTBs. On a reactor trip signal, the breakers will open, removing power from the control rod drive mechanisms. The control rods will then unlatch and drop into the reactor core due to gravity.

1. Motor Control Centre: a floor mounted assembly of one or more enclosed vertical sections having a common horizontal power bus and principally containing combination motor starter units. These units are mounted one above the other in vertical sections. The sections may incorporate vertical buses connected to the common power bus, thus extending the common power supply to the individual units. Units may also connect directly to the common power bus by suitable connections.
2. Reactor Trip Breakers correspond to some PWR plants (Westinghouse, Babcock&Wilcox, Combustion engineering and similar design).

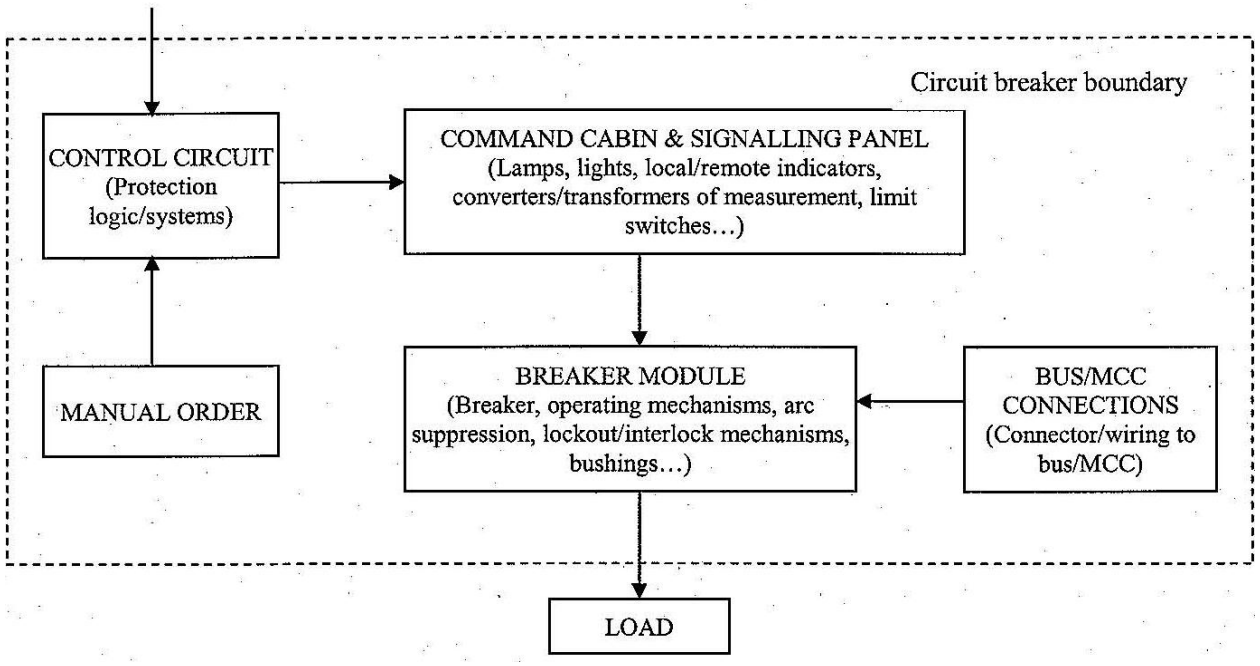
The following systems are to be evaluated. Their chosen voltage ranges match the voltage ranges of the IRS coding only approximately. Therefore the correspondence with the IRS system coding, added in parentheses, is only approximate:

1. Emergency Distribution System:
   - AC Low voltage, up to 1 000V (3.EC up to 600V)
   - AC Medium voltage, 1KV – 11KV (3.EB 600V to 15KV)
   - DC Low voltage (up to 600V) (3.EE)
2. AC Onsite Power Distribution System:
   - AC Low voltage, up to 1000V (3.EC up to 600V)
   - AC Low voltage, up to 1 000V (3.EC up to 600V)
   - DC Low voltage (up to 600V) (3.EE)
3. Reactor Protection System (Reactor Trip Breakers, low voltage) (3.IN)

Component Boundaries

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

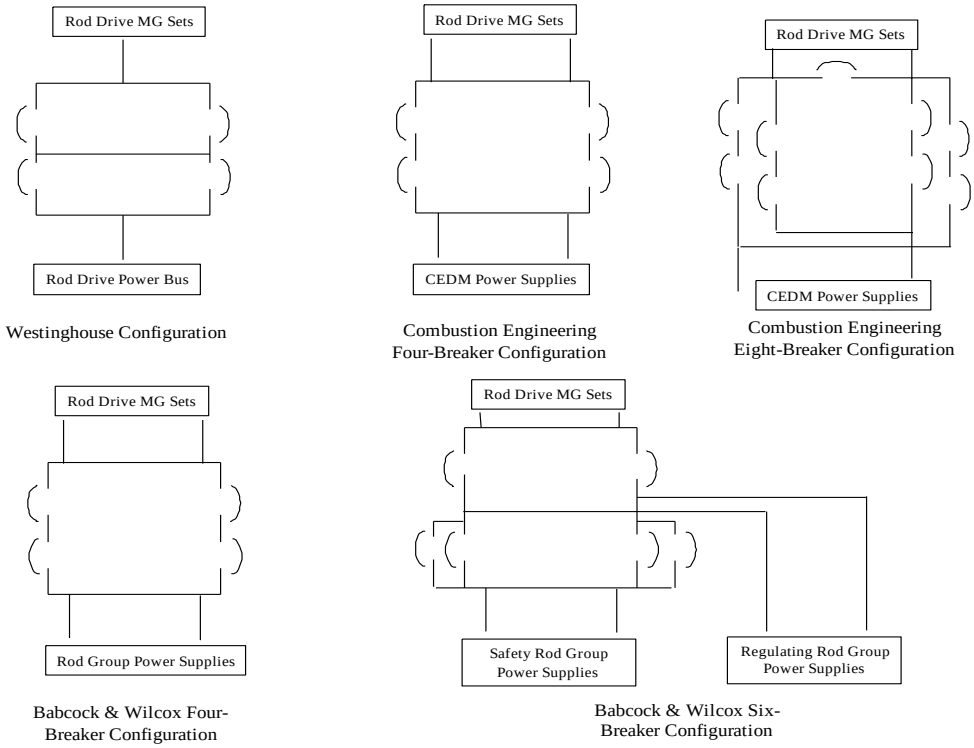
Figure 1.1 **Physical boundary of breakers**



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

Figure 1.2 shows the RTB arrangement for various vendors and designs.

Figure 1.2 **Reactor trip breakers**



Event Boundary

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

Basic Unit for ICDE Event Collection

The basic set for switching device/circuit breaker data collection is the observed population (OP).

Time frame for ICDE event exchange

The minimum period for the exchange should cover a period of at least 5 years, beginning no earlier than 1990.

Coding Rules and Exceptions

1. In general, the definition of the ICDE event is given in Section 2 of the General ICDE Coding Guidelines.
2. Some reports may discuss only one actual failure, and do not consider that the same cause will affect other Switching Devices/Circuit Breakers, but the licensee replaces the failed component on all switchgears/breakers as a precautionary measure. This event will be coded as incipient impairment of the components that did not actually fail.
3. Inoperability due to seismic or electrical separation violations will not be included, unless an actual failure has occurred.
4. Inoperability due to administrative actions will not be included as a failure if the report states that the component could have operated when it is required. (Example: a surveillance test not performed within the required time frame).

5. Guidance for CCF event interpretation (Field C7) and failure mechanism are in appendix A1.
6. A proposal for switching device/circuit breaker sub-components and subsystems is included in appendix A2.
7. In appendix A3, there are three classifications of switching devices and circuit breaker, according to the interrupting medium, function and voltage.
8. In appendix B1, there are some examples for complete, degraded and incipient failures, and situations without failure.

Functional Fault Modes

Essential failure modes

- Failure to Open (FO).
- Failure to Close (FC).
- Spurious Operation (SO).

(for some breakers only 1 or 2 of the 3 failure modes are relevant)

Successful RTB response to a reactor trip demand requires that the RTB open. The RTB is also required to remain closed until such a demand.

Failure to Open	Closed breakers that have a demand to open and fail to open. This includes manual operation, automatic operation such as load sequencing circuitry, RPS scram, and overcurrent/undervoltage conditions where the breaker fails to open.
Failure to Close	The breaker did not close or would not have been able to close if a close signal had been generated. In the case of RTB, they are tested to determine the closing time. If the closing time is too slow, the breakers must be worked on and re-tested. How far off of allowable closing time is considered a failure. The usual guidance here is if parts are indicated to be broken/worn/failed, and/or the closing time is greater than 10% over, a failure is recorded.
Failure to Remain Closed (Spurious Operation)	The breaker opened when it should have stayed closed or closed inadvertently, because of a breaker fault within the component boundary. Some reports state that the breaker was found in the tripped condition; these are considered spurious operation. Also included are spurious operations of the breaker due to personnel error, bumping the cabinet, or radio interference.

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

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

Appendix A

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	Symptom
CO	Corrosion (loss of insulation)
IEEC	Impairment due to Extreme Environmental Conditions
LDL	Loss/Deficiency of Lubricant
LSM	Loss/Deficiency of dielectric media (for ex. loss of SF_6, oil or vacuum)
PD	Pollution/Dirt (Loss of Insulation)
RMS	Relaxation of Mechanical Springs
SS	Spurious Signal in breaker auxiliary circuits Protection Systems
ST	Stress
TC	Thermal Cycling
WE	Wear
WF	Wiring Faults

Remarks:

- **CO - Corrosion**

  Examples

  Contacts

  The metallic surface of the current-carrying contacts can suffer pitting and corrosion. This corrosion can lead to an increase in contact resistance, high heating and, consequently, contact deterioration.

  Operating Mechanism

  Metallic pieces of operating mechanisms can suffer chemical attack, preventing an adequate performance.

  Metallic Frame

  The corrosion can affect the metallic frame/enclosure/case outside/inside surface should paint or other surface treatments fail

- **IEEC – Impairment due to Extreme Environmental Conditions**
  - ~ Outdoors/in the open air: storm, lightning, snow, rain, hail, ice, and salty atmosphere.
  - ~ Indoors: inadequate room cooling (higher or lower temperature than appropriate), moisture.

  This mechanism affects electric connections and insulators.

  Example:

  Contacts or Operating Mechanisms

  The metallic surfaces can be affected by moisture, temperature or salt ingress; even by the arcing process. These situations lead to corrosion, erosion, loss of conductivity (or electric resistance increase) and loss of electrical insulation.

- **LDL – Loss/Deficiency of Lubricant**

  Example:

  Operating Mechanisms

  Lubricants used in these mechanisms suffer ageing (e.g. grease hardening). This can prevent appropriate operation.

- **LDM – Loss/Deficiency of dielectric media**

  Example:

  Loss of SF_6 in a gas-filled interrupter compartment will lower the breaking capacity and can also cause a breakdown across open pole.

- **PD – Pollution/Dirt (Loss of insulation)**

  This mechanism affects electrical connections, arc chutes, bushings, insulators, etc.

  Examples:

  Contacts, Operating Mechanisms

  In general, the switching devices are well protected against ingress of dust or dirt. Dust accumulation inside the breaker produces a loss of electric insulation and, specifically in the contacts could lead to an increased resistance, which contributes to ageing by resistive heating. The presence of moisture could increase the rate of accumulation of dirt on the contacts. If, under these circumstances, the breaker is left for a long period without operating, this could cause the breaker to operate incorrectly.

- **RMS – Relaxation of Mechanical Springs**

  Vibrations, produced by opening/closing operations, can lead to an inadequate adjustment and slackness (even loss of mechanical engagement).

- **SS – Spurious Signal in Breaker Protection Systems**

  Example:
  A malfunctioning auxiliary contact in the circuit breaker.

- **ST – Stress**

  Significant stress can be produced by opening/closing operations. A high number of cycles can damage internal components. Failure of the damping device will enhance this damage; porcelain insulators are particularly prone to this.

- **TC – Thermal Cycling**

  Examples:

  Contacts

  The thermal cycling of the breaker conductor is caused by the varying currents experienced in normal and fault conditions. This cycling affects contacts if they are not adjusted, cleaned and lubricated correctly.

  Spring Charging Motor

  This element can be subjected to thermal cycling of insulation materials, because of a high temperature due to insufficient cooling in the breaker compartment. The most frequent failure is produced between the motor and the brush.

  Coils

  The high temperatures cause degradation of coil insulation materials in such way that perforation of the insulation occurs.

  Joints/Bellows

  The thermal ageing of joints (particularly those made in elastomeric materials) can produce a loss of insulation causing the joint to become less well fitting. Consequently, dust, water or dirt may enter, causing a decrease in insulation resistance and, probably, corrosion.

- **WE – Wear**

  Each time the breaker opens, the electric arc created cause deterioration of the contact area. The deterioration caused by the arc depends on the magnitude of interrupted current and the duration of the arc. Wear is also exhibited on the moving parts (i.e., the shaft). Wear, of course, can also affect other components such as compressor, solenoid, instrumentation, motor, etc.

- **WI – Wiring Faults**

  Failures of the cables and wires can lead to incorrect operation.

A2. Proposal for the Sub-components and subsystems

Code	Sub-Component	Sub-classification
AS	Arc Suppression	a. Arc Chutes b. Spring c. Magnetic Blow Coil d. Deflector Plates e. Plunger/Piston/Puffer/Bellow f. Cylinder g. Breaking Media Oil Tank h. Operating Media Air Tank i. Compressor
BE	Bearing	
BU	Bushings	
CB	Circuit Board	
CM	Closing Mechanisms	a. Spring b. Spring load motor c. Solenoid /coil d. Lever, handle wheel e. Electro-pneumatic devices f. Stored-energy devices g. Relays h. Latching mechanism
CO	Contacts	a. Main fixed contact b. Auxiliary fixed contact c. Main mobile contact d. Auxiliary mobile contact e. Arcing fixed contact f. Arcing mobile contact
CW	Connector/Wiring	
EN	Enclosure/Case/Frame	
IC	Interrupter Compartment	a. Oil b. SF6 c. Vacuum d. Air
IMR	Instrumentation/Monitors/ Recorders	
LIM	Lockout/Interlock Mechanism	
LMS	Load Motor Switch	
OM	Opening Mechanism	a. Spring b. Latching mechanism c. Solenoid/coil d. Lever, handle wheel e. Electro-pneumatic devices f. Stored-energy devices g. Relays

Code	Sub-Component	Sub-classification
PS	Protection Systems	a. Relays b. Solenoids c. Fuses/switches d. Alarms e. Sensor elements
TE	Terminals	
VA	Valves	

A3. Switching Devices and Circuit Breaker Classifications

Interrupting Medium

– Air Blast Circuit Breaker:
A circuit breaker using compressed air to force the extinction of the arc through an arc chute system. These breakers are used for switching protection & control application.

Several characteristics:

In general, air blast circuit breakers are high technology and robust equipment, with great electrical and mechanical endurance. Contact wear is low due to the short arc duration and low arc voltage.

– Air Magnetic Circuit Breaker:
A circuit breaker that uses air as insulating medium, and arc-chute system for dissipating the arc, a method of generating a magnetic field which forces the arc into the arc chute, and with possible assistance from an air puffer system to blow the arc into the arc chutes.

– Air Circuit Breaker:
This breaker is the most common type found in low voltage, relatively low current circuits for which the air serves as a suitable dielectric, preventing continued arcing between the contacts after they have parted. The contacts open and close in air at atmospheric pressure.

– Gas Insulated Switchgear (GIS):
GIS equipment is a type of metal-clad switchgear construction where all the switchgear components are located inside a sealed metal envelope filled with a gas. These components are used in switchyards of power plants. GIS has small space requirements and it is impervious to atmospheric contaminants.

Several characteristics:

High reliability; compactness; safety of operation; elimination of periodic maintenance & inspection; reduced installation time and costs; environmentally benign.

The most common GIS is the following:

SF_6 Gas Circuit Breaker: An arc extinguishing technology involves the use of Sulphur Hexafluoride gas.[4] They are much smaller than any other type of circuit breaker of equivalent power and are far less noisy than air circuit breakers.

Types:

- Two Pressure System: This breaker works by blasting high-pressure SF_6 gas across the arcing contacts during the interrupting process. SF_6 at a much lower pressure is used as the insulating medium for the interrupter tanks, columns and bushings.
- Single Pressure System: The puffer type breaker uses a moving piston or cylinder to compress the gas that is forced across the parting contacts during the trip sequence.

4. SF_6: Sulphur Hexafluoride, a gaseous dielectric for high and medium voltage power application, used as an insulator and/or interrupting medium. The highly stable SF_6 molecule consists of one central atom of sulphur (S) surrounded by 6 atoms of Fluorine (F).

– Vacuum Interrupter

An arc extinguishing technology. Features a pair of separable contacts enclosed in a vacuum-tight envelope. Since the environment inside the interrupter envelope is a vacuum, an arc cannot be sustained easily. These breakers operate on a principle different from other breakers because there is no gas to ionize when the contacts open. They are hermetically sealed; consequently, they are silent and never become polluted. They are used for switching protection & control applications.

Several characteristics:

- Excellent interrupting property (arcing time is less than 0.5 cycle).
- Compact design minimizes the installation space.
- Constant dielectric.

– Oil Circuit Breaker:

These breakers are composed of a steel tank filled with insulating oil.

Types:

- Minimum oil circuit breaker
- Bulk oil circuit breaker

– No Interrupting Medium.

Functions

- Switchgear/Bus/MCC Tie Breaker.
- Switchgear/Bus/MCC Feeder Breaker.
- Switchgear/Bus/MCC Load Breaker.
- Reactor Trip Breaker.

Note: the DG breaker is included within its component boundary

Voltage

– Medium voltage:
These components consist of air-magnetic, oil, and vacuum circuit breakers which operate in the range of 1 000Vac to 11KVac.

– Low voltage:
Low voltage circuit breaker typically operates at 1000Vac and at 600Vdc and below. There are three types:

- Molded Case Circuit Breakers: These components are available in a wide range and are generally used for low-current, low energy power circuits. The breakers have self-contained overcurrent trip elements.
- Insulated Case Circuit Breakers: These components are molded case breakers using glass-reinforced insulating material for increased dielectric strength. In addition, they have push-to-open button, rotary-operated low-torque handles with an independent spring charged mechanism providing quick-make, quick break, protection.
- Heavy Duty Power Circuit Breakers: These components employ spring operated, stored energy mechanisms for quick-make, quick-break manual or electric operation. Generally, they have draw-out features whereby individual breakers can be de-energized for maintenance purposes.

Appendix B

B1. Failure Examples

Complete Failures

Failure to Open/Close:

Switchgears/Breakers in general:

- Auxiliary contacts fail preventing the actuation of the switchgear/breaker or contacts fail to change the switchgear/breaker position (extracted/inserted).
- Opening/closing mechanism (spring, latching mechanism, solenoid/coil, lever, handle wheel, electro-pneumatic devices, stored-energy devices, relays) fails preventing the actuation of switchgear/breaker.
- Incorrect wiring in the power supply or in the control circuit of the component preventing its actuation.
- Misadjustment, breakdown or deterioration of the limit switches preventing the operation of the component.
- In a specific NPP design, loss of function of electronic-logical cards/modules (e.g. modules for priority control or for control interface in KWU NPPs) necessary for opening/closing operations.

Reactor Trip Breakers. In addition to the above examples, the following cases apply to the failure to open for these components:

- Electrical failures: continuity fault in the trip circuit, fuse blown, shunt trip coil burned or opened, inadequate operation of the undervoltage trip coil (out of the voltage limit).
- Mechanical failures: opening pawl seized up, break of opening springs.

Spurious Operation

- Failures in contacts, relays, closing coils (that must be energized) leading to the opening of the component when it is closed.
- Actuation of the protections not required (e.g., overcurrent due to adjustments) or spurious open/closure of the component when it is closed/opened.
- In a specific NPP design, loss of function of electronic-logical cards/modules (e.g. modules for priority control or for control interface in KWU NPP´s) causing a spurious actuation.

Degraded/Incipient Failures

- Time exceeded in opening/closing process over the normal observed, without endangering its function. (A recommended criterion is the following: If parts are indicated to be broken/worn/failed, and/or the closing time is greater than 10% over, a failure is recorded).
- Spring charging motor is continuously operating, but the detection of event is before the motor failure.
- Not simultaneous closure of the contact of all phases.
- Detection of fires or defective contacts before the component failure.
- Failures in the interlock mechanism (contacts or relays) which generate permissive signal or actuations for other equipments.
- Inadequate contact surface (hot spots or flaring areas due to contacts bent, dirty or burnt), without endangering its function.

Situations without failure

- Failures in signalling lights, such as those signalling the component state or failures of the manoeuvring meter.

- Failures induced by the PMs are not failures until the equipment is placed back in service, i.e., unable to rack the breaker back in, stab pins bent on closing, etc.
- Preventive maintenance (PM) actions such as cleaning, painting or grease replacement are clearly not failures.
- Spurious Indication (e.g. indicates wrong state)

ICDE

International Common-Cause-Failure Data Exchange **ICDE CG 09**

Component Coding Guidelines for Reactor Protection System: Control Rod and Drive Assemblies (CRDA)

Title: Coding Guidelines for Reactor Protection System: Control Rod and Drive Assemblies (CRDA)

Author(s): J.Tirira, A. Voicu, D. Rasmuson, T. Wierman, J. Dewailly, A. Oxberry, T. Mankamo and A. Kreuser

Issued by:

Reviewed by:

Approved by:

Abstract: This report defines the component-specific coding rules for Reactor Protection System: Control Rod and Drive Assemblies (CRDA)

Doc. Ref: Coding Guidelines

Confidentiality control: Confidential under OECD/NEA agreement

Distribution: WG, Project Web Site, Project archive

Revision control:

Version	Date	Version	Date
Draft 1.1	2002-11-15	Draft 1.6	2003-10-15
Draft 1.2	2002-11-30	Draft 1.7	2004-01-21
Draft 1.3	2003-03-13	Draft 1.8	2004-04-14
Draft 1.4	2003-04-22	Issue 1	2004-05-17
Draft 1.5	2003-09-11		

Component Coding Guidelines for Reactor Protection System:
Control Rod and Drive Assemblies (CRDA)

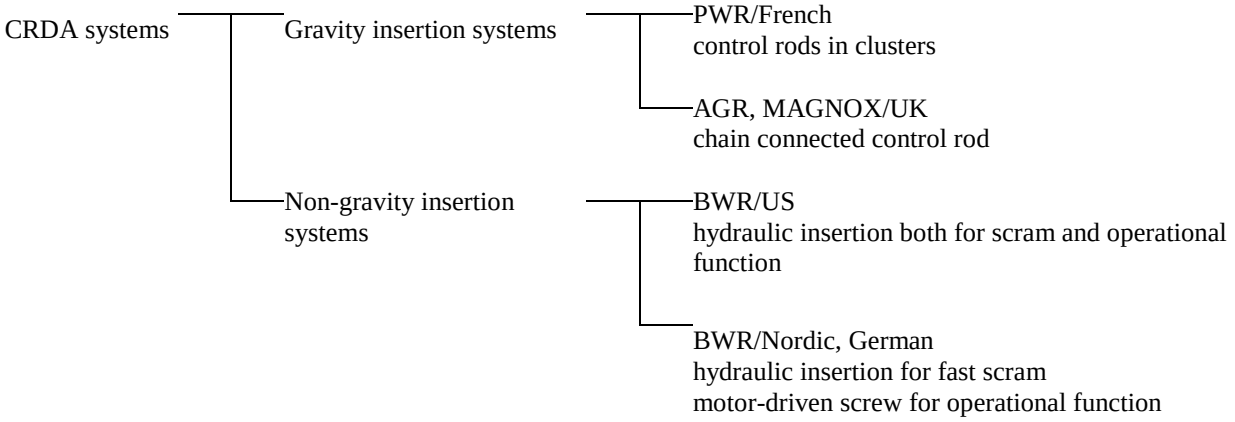
1. Introduction

The purpose of the Control Rod and Drive Assembly (CRDA, IRS code 3.AB) is to control reactivity when the reactor is in normal operating conditions and during rapid transients, and to provide sufficient additional negative reactivity for emergency operating conditions. The consequences related to the failure of the CRDA system depends on the initiator, plant state before scram and the needed effectiveness of the control rod population which is expressed by the minimal number of control rod clusters required at the position in the core cross section where the control-rod clusters failed to insert.

The nuclear power plant types concerned by collection of data on the CRDA are:

- Pressurized water reactors (PWR).
- Boiling water reactors (BWR).
- Magnox reactors.
- Advanced gas-cooled reactors (AGR).

The Coding Guideline describes selected basic designs that can be grouped according to the following tree:



In the opening sections of this document, the general description and component boundary of the different designs above are handled separately. As there are significant design differences among the reactor types, respectively, the general description of the component may not cover all possible variants in detail.

General aspects, which are common for the different designs will be discussed globally in a unique section providing general guidelines for data coding.

It is important to notice that CRDA system constitutes an ultra-highly redundant system, which places special requirements on the CCF analysis and event analysis. In order to conveniently use the foreign data, it is recommended to add a short system description document for each design in similar lines as the selected cases described here. If the CCF event has important design or operational factors outside the description in the guideline, they should be included in the event description to the extend available.

2. Pressurised Water Reactor

2.1 General Description of the Component

In view of the complex design and the impossibility to cover the substantial differences between manufacturers and design generations, this general description is focused on a generic description of French PWR designed by Framatome.

Control rods are cylindrical rods located inside control-rod channels in various locations in the fuel element assembly, in place of fuel rods. A cluster of control rods fastened to a spider at the top may have as few as five or as many as twenty absorbent rods. One control rod drive package is attached to each cluster of control rods.

The control-rod clusters enter the reactor pressure vessel through the top head. They withdraw upward and drop into the core by gravity during a scram.

All the control-rod clusters may be of the same type, or there may be two types with different types of absorbent rods:

- black control-rod clusters consisting of only absorbent rods and
- grey control-rod clusters, less absorbent than the black ones since some of the absorbent control rods are replaced by stainless-steel rods.

In addition, there may be two different functional sets of control-rod clusters:

- the shutdown set, made up of black control-rod clusters only and
- the control set, made up of both black and grey control-rod clusters.

Basically, the shutdown set is used to scram the reactor whereas the control set allows the control of nuclear power in operational state.

Control rod drives are mechanical, and depending on the manufacturer, are either continuously positionable or move in a series of discrete steps. All PWR rod drives, regardless of the manufacturer, incorporate a magnetic device, which is de-energized (via the scram or trip breakers) for scram.

The example drive mechanism in Figure 1 consists of stationary and movable grippers and electro-magnetic control coils; it moves the control-rod clusters step-by-step and allows all of them (both control and shutdown sets) to drop under their own weight for shutdown. Additional details are shown in Appendix 1.

Other designs of drive mechanisms involve the rotating of a magnetic field around the drive mechanism, which rotates the drive mechanism and moves the rod by a leadscrew. The rod is dropped by removing the field and unlatching the rod.

There are typically two or more methods of rod position indication: one basically counts the number of steps or turns of the drive mechanism although another independent system measures position by switches placed at intervals along the rod channel. These two methods are checked for agreement. In addition, most reactors have a separate “rod bottomed light”, which indicates that the control-rod cluster has passed a position in which it is considered bottomed. This can be as much as twelve inches above the actual bottom [1].

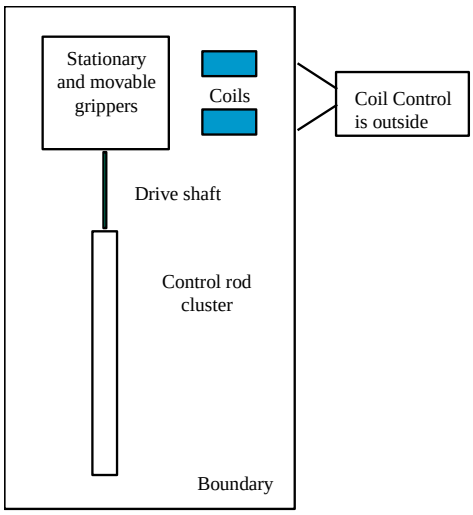
Component Boundaries

Control rod drive & rod components	
ROD	Control absorbent rod
CRC	Control rod cluster
CRD	Control Rod Drive

The CRDA system studied consists of two parts: all the control rod clusters (CRCs, themselves constituted by control absorbent rods (RODs)) and their drive mechanisms (CRD).

The number of CRDAs in the reactor core may vary from thirty-two to seventy depending on the design of the different plant series.

Figure 1. **PWR CRDA Component Boundaries**



For clarification: the trip breakers are the first elements outside of the component boundary of the CRDA.

3. Boiling Water Reactor

There are different realisations of the control rod drive system by different manufacturers. The description in chapter 3.1 is based on a US system. The description in chapter 3.2 is based on the Nordic design, which is similar to the general German design.

3.1 US design

General Description of the Component

The control rod drives enter the reactor vessel through the bottom head. The rods withdraw in the downward direction and so have a completely powered scram stroke against the force of gravity. Drives are hydraulic, and basically, they are hydraulic cylinders controlled by a “four-way valve with a closed center”. The hydraulic fluid is demineralised water. The “losed center” permits the control rod to be locked in any position.

The four “withdraw” and “insert” valves together make up the “four way valve” referred to above. Drive water pressure is 250 psi higher than reactor pressure. The cooling water pressure is 20 psi higher than reactor pressure and is adjusted to leak about 0.29 gpm, through each drive seal into the reactor. To insert a rod, the two insert valves are opened and high-pressure drive-water is then admitted beneath the drive piston. Speed is controlled by the insert speed-control valve. When the control rod reaches the desired location, the insert valves are closed again, and the latch is driven into place by its spring. Coolant flow continues to leak into the reactor vessel. The control rod is now locked into place both hydraulically and mechanically.

Rod withdrawal, however, is more complicated and is, therefore, programmed automatically. The insert valves are opened momentarily, the rod lifts, clearing the latch, and then the high drive-pressure, acting on the collet piston, drives the latch back out of the way. The insert valves close, the withdraw valves open and the rod now withdraws to the new position.

The safety function required of the drive packages is to scram the reactor. For this action, the drives are independent of any outside power source; all the necessary power is contained in the accumulator and the reactor vessel. On a scram signal the top of the piston is vented to an atmospheric header (Scram Discharge Volume) and the liquid in the accumulator, at 1500 psig (about 500 psi higher than the reactor vessel pressure), is admitted beneath the piston. The piston accelerates in the insert direction dropping the pressure in the accumulator. When the accumulator pressure drops below reactor pressure, the ball in the check valve shifts, closing off the accumulator, admitting reactor vessel pressure to complete the scram stroke. Accumulators are charged with nitrogen from gas cylinders and experience has shown that they need topping off about every six months; the actual recharging requires only ten minutes and does not interfere with plant operation. Nitrogen pressure is monitored and a pressure switch actuates an alarm whenever the accumulator needs recharging.

The accumulator, operating valves and interconnecting piping for each drive package are preassembled, and are tested at the factory. Each assembly shipped to the field then needs only pipe and electrical connections at the site. Additional details are shown in Appendix 2.

Control rod position indication is not continuous. Position is indicated every three inches by a series of glass-reed switches actuated by a magnet on the main drive piston.

Hydraulic fluid is supplied by one of two 100% capacity pumps. Excess fluid, not required for drive motion or cooling, is discharged into the reactor vessel. The fluid is supplied from the condensate storage tank.

Components and Component Boundaries for the US design

Control rod drive & rod components

SOV	Solenoid-operated valve	SDV	Scram discharge volume
AOV	Air-operated valve	ROD	Control rod
ACC	Scram accumulator	CRD	Control rod drive

The CRDs are hydraulic pistons connected to the bottom of the control rods. There is one hydraulic control unit (HCU) for each CRD/control rod. Some GE plants have a single, dual-coil SOV rather than two single-coil scram pilot SOVs. In addition, the number of scram discharge volumes can be either one or two.

Figure 2 shows a functional diagram of the mechanical portion of the General Electric RPS. Within each of the HCUs there are two scram pilot SOVs, two scram inlet/outlet AOVs, a scram accumulator, and various other components. If both of the scram pilots SOVs in an HCU are de-energized, then the air supply to the AOVs is bled off. Given loss of air, both the scram inlet and outlet AOVs open, allowing a path for scram accumulator water to flow to the closing side of the piston (forcing the control rod into the core) and the opening side of the piston water to drain to the SDV. As a sensitivity case, opening of only the scram outlet AOV was analysed. In such a case, reactor vessel water pressure (rather than accumulator water pressure) forces the control rod into the core. However, the rod insertion time is longer for this type of operation.

Figure 3 shows the SDV and associated level instrumentation and the backup scram SOVs. As discussed previously, either of the two backup scram SOVs can cut off the instrument air supply to the scram air header and bleed off the header. These SOVs require electrical power to energize to accomplish this.

The CRD water above the hydraulic piston is exhausted to the SDV. All of the CRDs exhaust to this volume. During normal operation, the SDV drain valves are open and the volume contains no water. However, if for some reason, during normal full-power operation, the drain valves were to close and the SDV started to fill with water, level switches (one-out-of-two-twice logic) trip the reactor before enough water collects to impact the CRDs. If the SDV were full of water before a reactor scram, then none of the CRDs could exhaust water above the hydraulic pistons, and none of the control rods would insert [1].

Figure 2. **General Electric RPS Simplified Diagram** (mechanical)

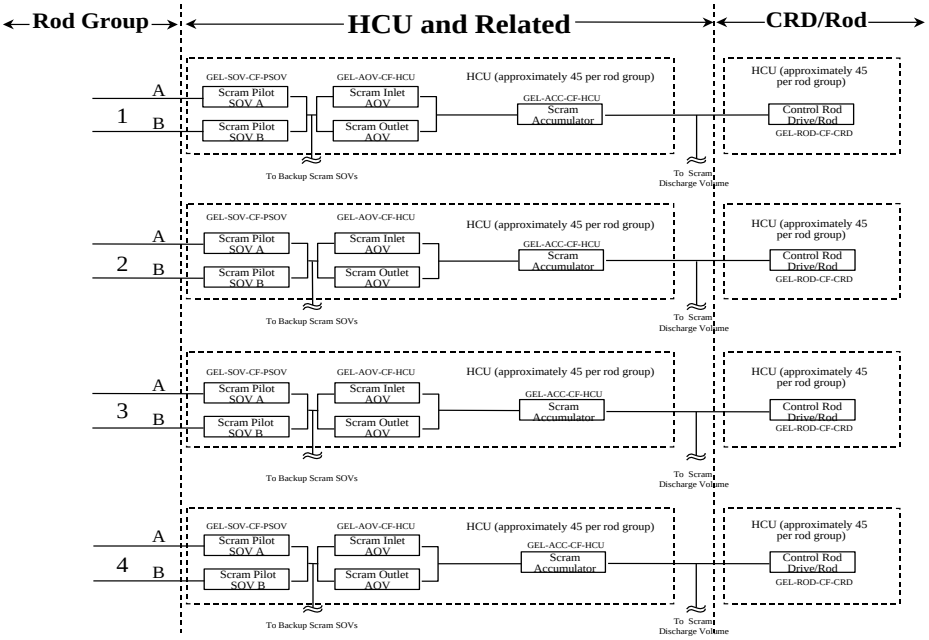
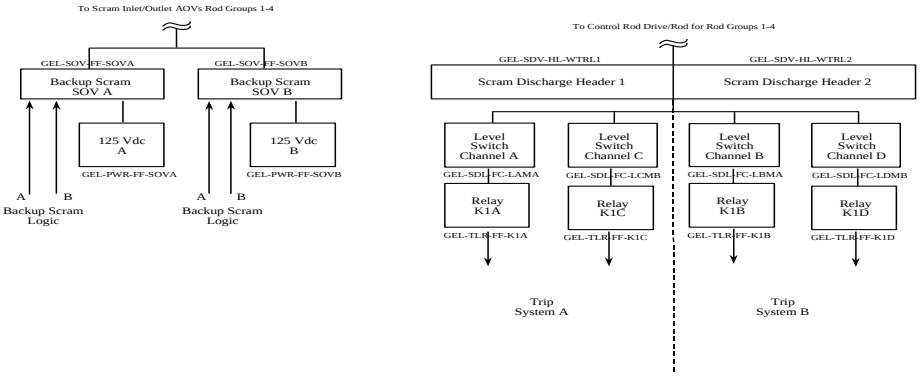


Figure 3. **General Electric RPS Simplified Diagram (SDV and backup scram SOVs)**



3.2 Nordic Design

This section describes the control rod and drive system of the Nordic BWR design, exemplified with the system description for Olkiluoto 1 and 2 plants. The design of the control rod and drive in German BWRs is similar (there are several variants both in the Nordic and German design). However, Nordic and German designs have some significant differences in the system providing the hydraulic driving force (high pressure water) to rod drives regarding internal configuration and redundancy, but components are similar. Figure 10 shows a schema of the hydraulic part of the reactor scram system of a German BWR. Figure 13 shows a schema of the corresponding system of a Nordic BWR, where it is a separate plant system named as Hydraulic Scram System (HSS) (Appendix 2).

The CRDAs of the Nordic BWR design are described in the next subsection, and HSS thereafter. The third subsection summarizes the component and boundary definitions.

Control Rod and Drive Assembly (CRDA)

In the Nordic BWR design the CRDA is constituted of a single absorbent rod (acronym ROD) along with drive unit (acronym CRD) (Figures 11-12 in Appendix 2).

The absorbent rod has a horizontal cross-section like a cross (+) and moves in the gap between four adjacent fuel channels. It is steered within the gap of the fuel channels and was separated in the original design from the fuel channels by guide plates, attached by screws. This design was changed because the detached screws and guide plates have caused jamming of control rods.

The control rod is inserted from bottom upwards into the core. The control rod shaft penetrates the bottom of the reactor vessel. The penetration is equipped with multistage sealing. The number of control rods varies between 109 and 169 in the Nordic BWRs. They are spread evenly across the core.

Briefly described, the drive has dual functions:

- Hydraulic piston function for fast insertion (fast reactor scram).
- Motor-driven screw insertion/withdrawal function (power regulation, normal reactor shutdown and start-up).

The normal full stroke time is about 4 seconds for hydraulic insertion and about 4 minutes for screw insertion. The screw insertion is credited for reactivity shutdown in slower transients.

The piston tube is connected to the rod shaft with a bayonet coupling (Figure 11). The lower end of the piston tube rests on the drive nut by the weight of the control rod. The drive nut can be moved upwards/downwards by the drive motor, which rotates the drive screw, providing the fine motion and accurate positioning of the control rod. In hydraulic insertion the piston tube is locked in the uppermost position. The latch is unlocked when the drive nut is driven up and reaches the lower end of the piston tube. The fast scram signal, so called SS-signal from the Reactor Protection System (RPS), which primarily actuates the hydraulic insertion, is automatically followed by an actuation command to screw insertion. The drive nut is then driven up to reach the lower end of the piston tube after a hydraulic insertion. In the case of failed hydraulic insertion the screw function may complete the insertion. However, the screw insertion is weaker in most jamming mechanisms in comparison to the hydraulic insertion. The hydraulic force of insertion is about ten times the weight of the control rod.

The drive motor is protected by slip coupling (so-called moment trip) against overloading in case of high friction or jamming).

The electric power supply to the drive motors is divided over four redundant diesel-backed buses. The electric power supply to the instrumentation and control circuits is divided over four redundant battery-backed buses. The CRDA component boundary with respect to electric power supply systems is as standard: the local contactors and protective devices are counted as part of the CRDA.

The scram signal bypasses any power regulation commands, minimizing the contribution of the Control System of Motor Drives with respect to failure of screw insertion in demand. The control circuits after RPS end relays are considered as part of the CRDA.

The position measurement serves power regulation and operational/test purposes, with practically no direct impact on the safety functions of the CRDA. The position of the control rod can be indicated with an accuracy of 1 %. Additional indications are provided to verify the fully inserted position and inform about the separation of the drive nut from the lower end of piston tube. The latter one is particularly important (for operational aims) in order to notice conditions when the control rod will not follow the drive nut but is jammed at withdrawal.

Hydraulic Scram System (HSS)

HSS provides hydraulic driving force to rod drives (Figure 13 in Appendix 2). It is constituted of identical redundant trains: the number of trains varies from 14 to 28 in Nordic BWRs. The CRDA groups connected to HSS trains are called “scram groups”. The CRDAs are selected to scram groups with the aim to have an efficient as possible distribution throughout the core, in order to minimize the influence of the failure of any single scram group.

The components of HSS are placed outside the reactor containment, except the internal isolation valve, which facilitates test and maintenance actions during normal power operation.

The only more specific design feature is the diversified configuration of the pilot valves in the scram valve: the four solenoid pilot valves are connected as 2 out of 4 logic in each scram valve. Consequently a problem with one pilot valve is not critical. The pilot valves receive signals from the RPS end relays that are outside the HSS boundary.

Components and Component Boundaries for the Nordic Design

The CRDA is constituted of a single absorbent rod (ROD) and dual-function drive (CRD). The component boundary of the CRDA is described in Figure 12.

Because HSS has different degree of redundancy, it has to be handled separately from the CRDAs in the Nordic BWR design (one HSS train is connected to many CRDAs, and the concerned rods are dispersed across the reactor core). The main components of the HSS train are the following (Figure13 in Appendix 2):

- Nitrogen pressure tank and scram water tank, and the connecting nitrogen and water supply lines, and local control equipment.
- Air-operated scram valve (normally closed) between nitrogen pressure and scram water tanks.
- Non-return valve.
- Manual closing valve (normally open).
- Air-operated external isolation valve (at the containment boundary, normally open).
- Non-return, internal isolation valve (at the containment boundary).

The HSS trains have shared equipment for nitrogen supply and water makeup/outlet. Owing to fail-safe design and efficient on-line monitoring these shared parts have only a very small contribution to the reliability of scram function. The component boundaries for HSS and connected systems follow the standard definition for the valves, and instrumentation and control equipment [2]. The interface of the HSS train and the CRDAs is at the scram water inlet pipe (Figure13). The non-return valve at the inlet of rod drive is a part of CRDA (Figure 11).

The component definitions and corresponding failure mode definitions are summarized in Section 6.5.2 in a harmonized way covering Nordic, German and US BWR design magnox reactors

4. Magnox Reactors

4.1 General Description of the Component

Control rods are cylindrical rods located inside control rod channels in various locations in the core. Unlike PWRs, the control rod channels are entirely separate from the fuel assemblies.

For Magnox reactors, control rods enter the pressure vessel through the top head. Each reactor is equipped with control rods which are essentially of two types; “black” rods (also called “bulk” or “coarse” rods) and “grey” rods (also called “trim”, “sector” “regulating” or “zone” rods). Black rods are more absorbing than grey rods. Rods of both types are used to control the reactor. However, when the reactor is at steady load, black rods are not normally moved and fine control of reactivity is achieved by movement of the grey rods. The rods in each group are distributed throughout the core. All control rods can be driven manually from the control room. Some grey rods on some plants can also be driven automatically. Some stations break down the sets of rods further, for example Oldbury differentiates between “trim” control rods and “sector” control rods, both of which are grey.

All black and all grey rods are inserted into the core to trip.

Figure 14 in Appendix 3 shows a schematic of a control rod and average dimensions; actual dimensions vary according to core depth. The wire “rope” or chain, used to suspend the rod can be seen at the top of Figure 14.

There are a number of different designs of actuator used in Magnox plants. Each control rod is raised and lowered by motor-operated winding gear driving through a gearbox. The actuator also contains one or more clutch mechanisms and an adjustable brake. The braking mechanism varies between different reactor designs.

The trip system consists of contactors located in the supply lines to the windings of the control rod motors. These contactors are held closed (energised) during normal reactor operation. If the contactors are de-energised (automatically, manually or through loss of power), the rods drop into the core under gravity to trip the reactor.

The reactor is protected by a number of reactor protection circuits known as guardlines. The rod trip relays provide the link between the guardlines and the control rod trip contactors. The relays de-energise the control rod trip contactors if the normal guardline 2oo3 trip logic or the diverse guardline trip logic is satisfied, or the manual trip push button is operated.

Magnox reactors have another rod shutdown mechanism, ("safety" rods) which is entirely independent of the black and grey control rods. The set of safety rods have sufficient neutron absorption properties to shutdown the reactor and hold it shutdown. They are not used to control the reactor or for planned controlled shutdown. They are normally latched out of the core including during reactor shutdown periods. Various diverse mechanisms are associated with the latches, so that the occurrence of certain properties cause de-latching and the drop of rods into the core under gravity. Some of these latch mechanisms are mechanical, such as bellows, causing trip on loss of reactor pressure. Safety rods may be inserted into the core during shutdown conditions when black or grey control rods are removed for maintenance.

4.2 Magnox Component Boundaries

Control rod drive and rod components	
ROD	Control absorbent rod
CRD	Control rod drive/actuator

For control rods

The CRDA system studied consists of two parts: all rods (RODs) and all control rod drives (CRDs). CRDs are constituted of all ropes or chains (ROPEs) and all actuators.

The trip contactors can be said to be within the boundary of the CRD. The guardlines and the guardline end relay, which control the removal of power from the contactors of the motor are outside the component boundary.

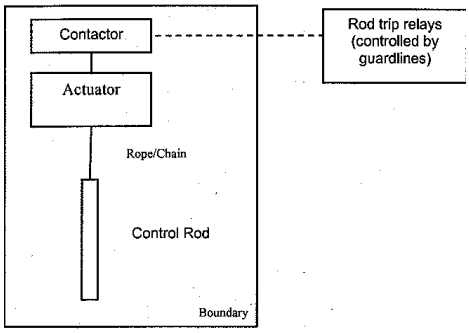
There are approximately 100 CRDAs in a reactor core, but this number varies with the individual plant design and size.

For safety rods

The CRDA system studied consists of two parts: all rods (RODs) and all control rod drives (CRDs). CDRs are constituted of all ropes or chains (ROPEs), all latches (LTCHs) and all latch mechanisms (LMs).

The number of safety rods in a reactor core varies from 10 to 20.

Figure 4. **Magnox CRDA Component Boundary**



5. Advanced Gas Cooled Reactor

5.1 General Description of the Component

Control rods are cylindrical rods located inside control rod channels in various locations in the core. Unlike PWRs, the control rod channels are entirely separate from the fuel assemblies.

In AGRs, control rods enter the pressure vessel through the top head. Each reactor is equipped with black and grey control rods. Black rods are more absorbing than grey rods. Both black and grey rods are the same dimensionally and structurally, except that black rods contain an extra boron insert.

Groups of control rods are assigned names which reflect their use. When the reactor is at steady load, "bulk" or "coarse" rods are not normally moved and fine control of reactivity is achieved by movement of the "regulating" or "trim" rods. Rods of both types are used to control the reactor during start up and controlled shutdown. Bulk/coarse rods are black and regulating/trim rods are grey. At Dungeness B (the first design of AGR), one rod per reactor zone is under direct automatic control to counteract the minute to minute perturbations of the reactor. These rods are named "sector" or "zone" rods. The remaining grey rods (termed "trim" rods) are under manual control. All later AGRs have full automatic control of all regulating rods, individual rod positions being determined by averaging a number of local channel outlet temperatures.

The control rods usually consist of a number of cylindrical steel sections linked axially by articulating joints (Figure 15 in Appendix 4). These joints would allow the control rods to enter in an extreme condition in which the core became slightly distorted. Some stations have "sensor" rods, which have fewer articulating joints. Sensor rods are inserted into and withdrawn from the core periodically to detect any gradually developing guide tube misalignment. Sensor rods are a subset of the bulk or coarse black rods.

In AGRs, a subset of the normal control rods may be designated as "safety" rods. These are grey rods, and function as regulating rods while the reactor is on load.

To trip, all control rods drop into the core under gravity, by the main guardlines, diverse guardlines, or manual push-button. Following successful shutdown, the safety rods are withdrawn from the core. The remaining rods provide ample shutdown margin. If following shutdown, reactivity unexpectedly starts to rise again (e.g. due to incorrect refuelling), the safety group will trip into the core, initiated by the shutdown guardlines.

Each control rod is raised and lowered by motor-operated winding gear driving through a gearbox. The actuator also contains a torque-limiting clutch, an electromagnetic clutch, suspension chain storage, rod position indication and limit switches (Figure 5). A hand wind drive is fitted to lift the rod when the power supplies are removed prior to maintenance.

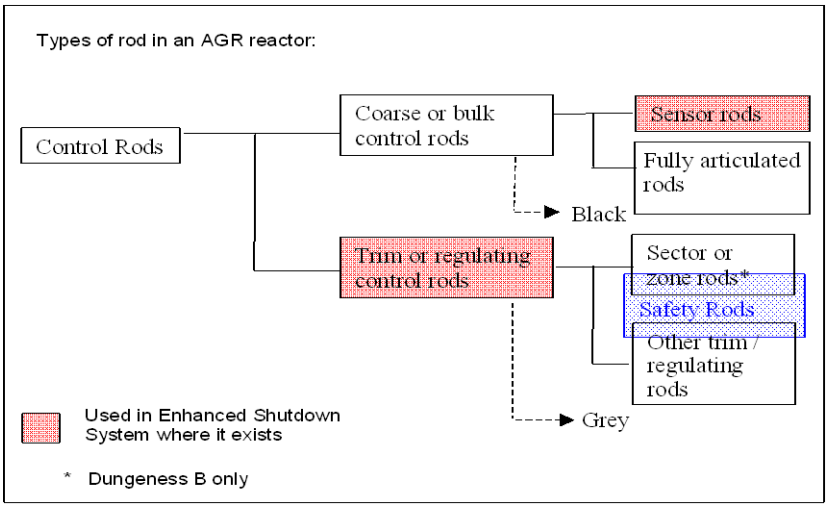
To trip the reactor, power supplies are removed from the electromagnetic clutches within the control rod drive mechanisms such that the control rods drop into the core under gravity.

When the clutch is de-energised, the insertion rate of the rod is controlled by a brake. Braking limits the stress in the chain suspension and gearing.

The reactor is protected by a number of reactor protection circuits known as guardlines. If the guardline logic is satisfied, power supplies to the control rod clutches are removed.

Two AGR stations (Dungeness B and Hinkley Point B) also each have a secondary system, called the Enhanced Shutdown System whereby the grey and sensor control rods are motored into the core if they fail to fall in under gravity. This system is designed to mitigate failure of the clutch to release, either mechanically or due to electrical faults, and the motors effectively double as the braking mechanisms. The normal control rod motors are used in the Enhanced Shutdown System, although at Dungeness B the motors are run at twice their normal speed. The grey rods alone provide sufficient absorbency for short term shutdown. Long-term hold-down is provided by a vaporised nitrogen system which may take as much as an hour to start up. The sensor rods are included in the Enhanced Shutdown System as a back-up to allow more time to start up the Nitrogen system.

The other AGRs do not require Enhanced Shutdown Systems as they have rapid-acting secondary shutdown systems using nitrogen gas under pressure, backed up by longer term tertiary systems using boronated glass beads.



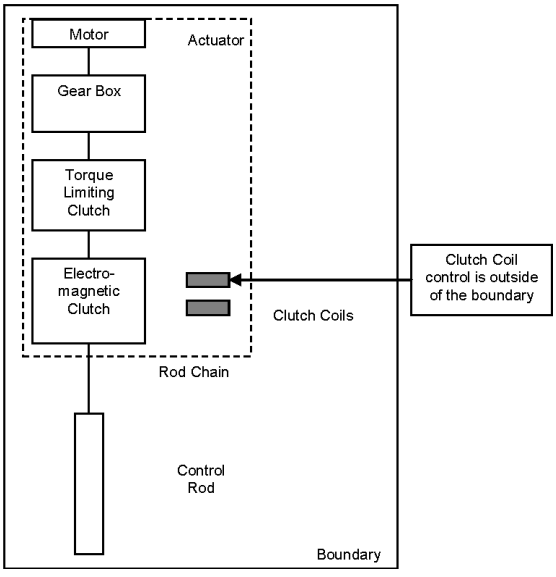
5.2 AGR Component boundaries

Control rod drive and rod components	
ROD	Control absorbent rod
CRD	Control rod drive/actuator

For control rods, the CRDA system studied consists of three parts: all rods (RODs) and all control rod drives (CRDs). CRDs are constituted of all ropes or chains (ROPEs) and all actuators (CRDs). The electromagnetic clutches are within the boundary of the CRD. The guardlines and the guardline end relay, which control the removal of power from the coils of the electromagnetic clutch are outside the component boundary.

There are approximately 100 CRDAs in a reactor core, but this number varies with the individual plant design and size.

Figure 5. **AGR Component Boundary**



6. Specific Coding Rules for CRDA Data Collection

6.1 Event Boundary

The CRDA system has two separate and distinct missions: safety and operational missions. The *safety* mission of the CRDA system is to insert a substantial quantity of absorbent material into the reactor core, by allowing it to drop under the effect of gravity (PWR, Magnox and AGR) or driving the rods into the reactor vessel under hydraulic pressure (BWR) when there is an automatic or manual reactor shutdown signal, in order to terminate the nuclear reaction and make the reactor sub-critical.

The *operational* mission of the CRDA system is to ensure an acceptable distribution of power in reactor core during the operational state. This data collection effort is concentrated on the data collection for the safety mission. Nevertheless, most of the CRDA components are involved in both safety and operational mission. The failures having affected the operational mission being related to failure mechanisms which can affect also the safety mission should be collected.

Failure of the component CRDA to fulfil its safety mission involves non-insertion or delayed insertion of one control-rod cluster into the reactor core.

6.2 Basic Unit for ICDE Event Collection

The basic set for control rod and drive assembly event collection is the observed population of all CRDAs and the optionally covered components of the systems or system parts providing the hydraulic driving force in the BWRs.

6.3 Time Frame for ICDE Event Exchange

The minimum period of exchange should cover a period of 5 years. The recommended screening time window for the CCFs in reactor scram is the time cycle defined by the refuelling outages and/or overhaul outages.

6.4 General Coding Rules and Exceptions

In general, the definition of the ICDE event given in Section 2 of the General ICDE Coding Guidelines Revision 4 applies.

Plant state at the event detection should be described in event description because it can have a substantial bearing for the significance of the failure in scram systems. The failure cases observed in post-maintenance tests in overhaul outage or in subsequent start-up tests may not be relevant for the power operation state.

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

Some reports discuss only one actual failure, and do not consider that the same cause will affect other CRDAs, but the licensee replaces the failed equipment on all CRDAs concerned as a precautionary measure. This type of event will be coded as a CCF, with an incipient failure value for the components that did not actually fail.

The length of the impairment vector could be equal to the size of the exposed population; however, in view of the high number of CRDAs, only the information on the impairment status of each failed component should be coded using the usual ICDE codes (C, D, and I).

Administrative in-operability that does not cause the control rods to fail to function will not be included as failures. An example is a surveillance test not performed within the required time frame.

In-operability due to human error or erroneous calibration/set up will be included (in either ICDE or independent event coding).

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

6.5 Functional Safety Mission Fault Modes

This section describes separately the mission failure modes for both gravity insertion systems (PWR, Magnox and AGR) and the hydraulic/screw insertion systems (BWR). The system dysfunctions preventing the system from fulfilling its safety missions and their possible causes are described in Section 6.5.3

Gravity insertion systems (PWR, Magnox and AGR)

Failure of the system to fulfil its safety mission involves non-insertion or delayed insertion of one control-rod cluster/rod into the reactor core.

The two failure modes considered are:

- Essential failure modes:
  Failure to completely insert (FCI)
- Several countries also have:
  High (large) control-rod cluster/rod insertion time exceeding Technical Specifications (HIT-G)

For gravity insertion systems the data can be collected for the main components, using the specifications of components, component types and corresponding failure modes as summarized in the following table.

Table 1. **PWR Components and Failure Modes**

System part	Component	Component type	Failure modes
CRDA (Gravity)	ROD: Absorbent rod	General (All designs)	FCI; HIT
	CRC: Control rod cluster	General (PWR)	FCI; HIT
	CRD: Control rod drive	General (All designs)	FCI; HIT

Non-gravity insertion systems (BWR)

The considered failure modes for the CRDAs of BWR are the same two as those described for gravity insertion systems (FCI and HIT). In particular, for BWRs with dual-function drives the failure modes related to insertion are decomposed as following [2]:

Hydraulic insertion

- Essential failure modes: Failure of the hydraulic insertion function (FCI-H).
- Several countries also have: High insertion time (HIT-H).

Electromechanical insertion

- Essential failure modes: Failure of the electromechanical insertion function (FCI-M).
- Several countries also have: High insertion time (HIT-M).

Hydraulic and electromechanical insertion

- Essential failure modes: Failure of both hydraulic and electromechanical insertion function (FCI-B).
- Several countries also have: High insertion time (HIT-B).

The data can be collected separately for the rod component (ROD) and drive component (CRD), or optionally the CRDA (ROD+CRD) can be handled as one functional component (a usual practice in PSA modelling). In the latter option the event description should tell the failure location for qualitative analysis aims.

The data collection for BWRs can be extended to comprehensively cover the hydraulic part of the scram system, i.e. hydraulic driving force supply. In this part the data can be collected for the main components, using the specifications of components, component types and corresponding failure modes as summarized in Table 2.

Table 2. **BWR Components and Failure Modes**

System part	Component	Component type	Failure modes
CRDA (Non-gravity)	ROD: Absorbent rod	General	According to CRD type
	CRD: Control rod drive	HH: Hydraulic both for fast insertion and operational function	FCI-H HIT-H
		HM: Hydraulic fast insertion and motor-driven screw for operational function	FCI-H, M, B HIT- H, M, B
Hydraulic driving force supply	PIV: Pilot valve	SOV: Solenoid operated valve AOV: Air-operated valve	FO, FC
	SCV: Scram valve	AOV: Air-operated valve HOV: Hydraulic operated valve	FO, FC
	CLV: Closing valve	AOV: Air-operated valve HOV: Hydraulic operated valve MCV: Manual closing valve	FO, FC, also IC for normally open CLV
	ISV: Isolation valve	AOV: Air-operated valve NRV: Non-return valve	FO, FC, also IC for normally open ISV
	ACC: Accumulator	SCW: Scram water tank NTR: Nitrogen pressure tank	Failure to supply hydraulic driving force
	SDV: Scram discharge volume	General type	Failure to supply hydraulic driving force

Essential failure modes for the valves are:

1. Failure to open (FO).
2. Failure to close (FC).
3. Inadvertent closure (IC).

(depending on component type only one or more of these failure modes are relevant)

Due to the differences in the configuration and internal redundancy of hydraulic scram system the consequences of component failures and multiple failures may need to be specifically described with respect to rod insertion function. Depending on the case this information can be provided in the separate system description notebook, in OP definition field G1 or in event interpretation field C7.

In the case of a design such as Nordic BWR where the hydraulic scram system is a separate system (HSS) constituted of redundant, largely independent trains, the data can be collected in train-wise manner, i.e. a HSS train can be considered as one functional component (a usual practice in PSA modelling). The functional failure mode applicable to HSS train is "failure to supply hydraulic driving force". This practice is recommended because not many CCF events have affected the HSS in Nordic BWRs. The closer location of failure can be described in the event text for qualitative analysis aims. The shared parts of the trains (nitrogen supply and water makeup/outlet) can be handled as a special source location of CCFs (very unlikely to significantly affect reactor scram function owing to fail-safe design and efficient monitoring).

System failure causes

Described below are the system dysfunctions preventing the system from fulfilling its safety missions (FCI and HIT), as well as their possible causes.

Table 3. **CRDA Failure Causes**

Code	Failure cause	Applies to	Failure mode	Root cause	
				Code	Description
DEF	Deformation of fuel assemblies	PWR BWR	HIT/FCI	C	State of other components
MIS	Misalignment between the reactor core and the steel structure above it	AGR MAGNOX	HIT/FCI	C	State of other components
ARS	Broken anti-rotation screw	PWR	FCI	D	Design manufacture, construction inadequacy
SFM	Sticking of the freewheel mechanism in the control rod actuator	AGR MAGNOX	FCI	D P	Design manufacture, construction inadequacy Procedure inadequacy
CSR	Contact shoulder/drive rod	PWR	FCI	P	Procedure inadequacy
SCC	Swelling/cracking of control rod casings	PWR AGR MAGNOX	FCI/HIT	A	Abnormal environmental stress
CRB	Control rod breakage	All designs	FCI	A	Abnormal environmental stress
FOB	Foreign object	All designs	FCI	O	Other
DEC	Decrease in rod neutron absorbency	AGR MAGNOX	FCI	D A	Design manufacture, construction inadequacy Abnormal environmental stress
IAR	Incorrect adjustment of rope length	AGR MAGNOX	FCI	P	Procedure inadequacy
IAB	Incorrect adjustment of brake	AGR MAGNOX	HIT	P	Procedure inadequacy
MTR	Moment trip of electromechanical drive function (slip coupling or over current protection)	BWR (CRD type HM)	FCI-M	I	Internal to component, piecepart

Deformation of fuel assemblies

Fuel assemblies may deform due to creep induced by irradiation, thermal, mechanical and hydraulic loading, and their mutual interaction. Assemblies with significantly deformed guide tubes are likely to have longer rod drop times (HIT), or even to have rods jam before reaching the bottom (FCI).

Broken anti-rotation screw on stationary gripper of control-rod drive mechanism

The screw is to prevent rotation of the two parts of the articulated section of the stationary gripper. Screw breakage and ejection of the screw head into the space between the plunger and the housing can jam the stationary gripper. If the gripper jams, it prevents the control rods falling when they are required to (FCI).

Contact between the shoulder of the protective sleeve of the drive rod and the lower edge of the upper bevel of the rod support plate

This risk (FCI) concerns only clusters in very high positions, i.e. inserted only into the edge of the core, and whose drive rods are curved (i.e. within the manufacturing tolerance); it disappears when the protective sleeve of the drive rod is inserted into the bore of the support plate (a modification of the Technical Specifications prohibiting to place the control rods in a very high position resulted in elimination of the discrepancy).

Swelling and/or cracking of control-rod casings

This example of failure cause may result from the behaviour of the neutron absorber. This may eventually cause loss of part of the neutron absorber or jamming of one or more control-rod clusters (FCI).

Control-rod breakage

Control rod clusters can start vibrating as a result of complex flows inside the upper internals. Because of these vibrations, the control rods come into contact with the guide system (guide plate, continuous

guidance, etc.). This causes wear of the control rods and some guide parts. Excessive wear of a control rod can result in breakage due to fatigue cracks initiating in and propagating from the zone affected. The piece of broken rod may jam at any altitude across the tube guide and prevent the insertion of the intact piece of rod. Also, a ruptured control rod which stays in the core when the control-rod cluster is withdrawn reduces the amount of available anti-reactivity of the control-rod cluster (FCI).

Jamming due to detached component parts

Foreign objects, for example detached component parts such as slide plates/bolts/screws and fuel channel screws, have caused several insertion failures when migrated in a position between rod and guide tube, or between rod and fuel channel in the Nordic BWRs. These cases include a few critical failures of the hydraulic insertion (FCI-H) and many critical failures of screw insertion (FCI-M), and one event where both functions failed (FCI-B) according Nordic BWR experience up to 1995 [4].

Moment trip of electromechanical drive function

The most frequent failure type of screw insertion (FCI-M) is the moment trip, i.e. slip coupling or overcurrent protection has stopped the operation. There have been many different causes such as accumulation of crud and component wearout, which often have contributed in combination, and also caused actual CCFs in the Nordic BWRs [4].

Example of failures not to be collected

Events with insignificant risk for the CRDA safety mission shall not be included in the data collection. Those events affecting only the operational functions, with no or negligible implications for the safety insertion should be screened out, as for example:

- Control rod (or control rod cluster) is jammed at fully inserted position, and the failure mechanism does not have potential to cause failure to insert. An example of a shared failure mechanism in this regard is foreign object such as a detached screw head.
- Failure to withdraw, again with the condition that the failure mechanism does not have potential to cause failure to insert. An example of a failure mechanism which can affect both insertion and withdrawal is foreign object such as a detached screw head.
- Failures in the instrumentation such as position measurement without impairing the safety insertion.
- The monitored failures in BWR Hydraulic Scram System (separate system), e.g. external leakages, can be screened out, assuming that they have insignificant impact on the safety insertion function.

6.6 Guidance to Describe and Codify CCF Events

The event description should always clearly indicate the position of jamming with respect to the fully inserted position and the insertion time if slow, with respect to the required insertion time, as well as the type of CRDAs concerned (black/ grey, shutdown/control) when there is diversification among CRDAs. The event description should further give information on the relative position of impaired rods such as e.g. “neighboured rods” or “only outer rods concerned” or “no radial core-position related correlation between impaired rods”.

Regarding event codification the following examples are given for the failure mode “failure to completely insert”:

- Complete failure: control rod incompletely inserted before entering in the dashpot,
- Degraded failure: control rod incompletely inserted in the dashpot,
- Degraded failure: broken head of anti-rotation screw is detected in close circuit television inspection and removed in vessel head replacement
- Incipient failure: control rod is dropping without bounce in a drop time test

7. References

[1] Keneth C. Lish, Nuclear Power Plant Systems and Equipment, Industrial Press, Inc.

[2] T-BOOK 5th edition, Reliability data for Components in Nordic Nuclear Power Plants, edited by the TUD Office SwedPower, AB in 2000

[3] Reliability Study: General Electric Reactor Protection System, 1984-1995. Prepared by S.A.Eide, *et. al.*, Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.3., February 1999.

[4] Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems at the Swedish and Finnish BWR plants. Prepared by T. Mankamo, Avaplan Oy for the SKI. SKI-Report-96:77, December 1996.

Appendix 1.

PWR Schemas

Figure 6. **Cutaway View of a PWR Control Rod Assembly**

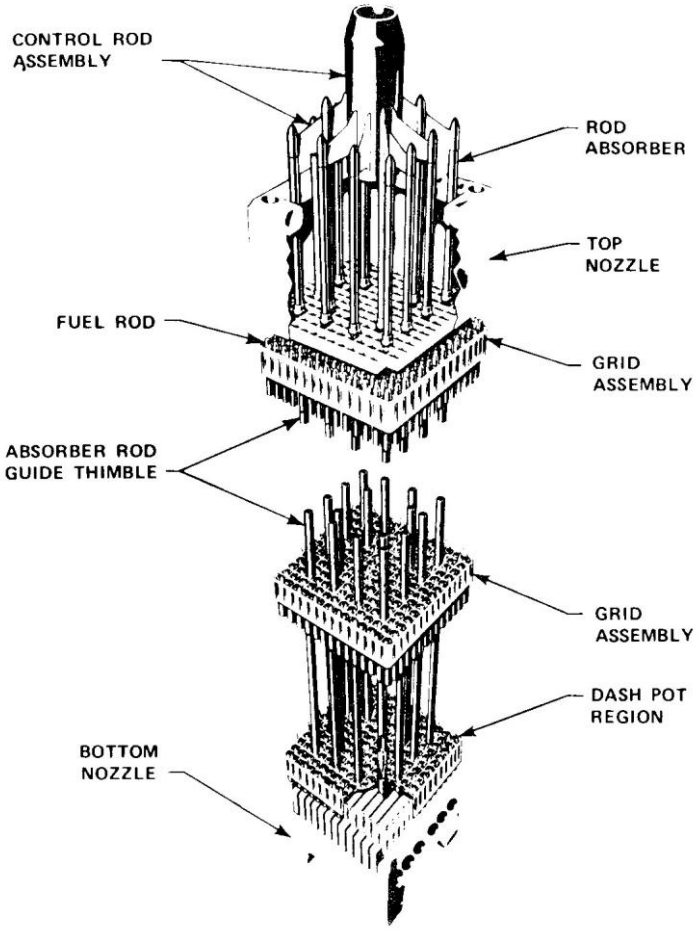


Figure 7. **PWR CRDM Magnetic Jack Arrangement**

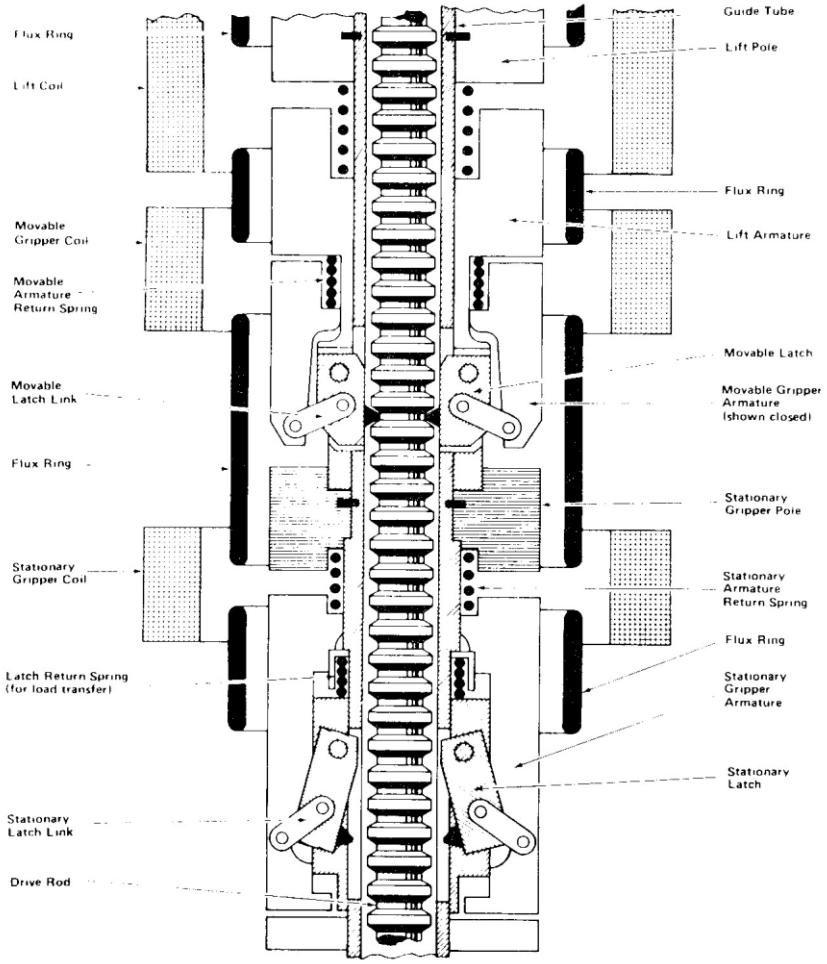
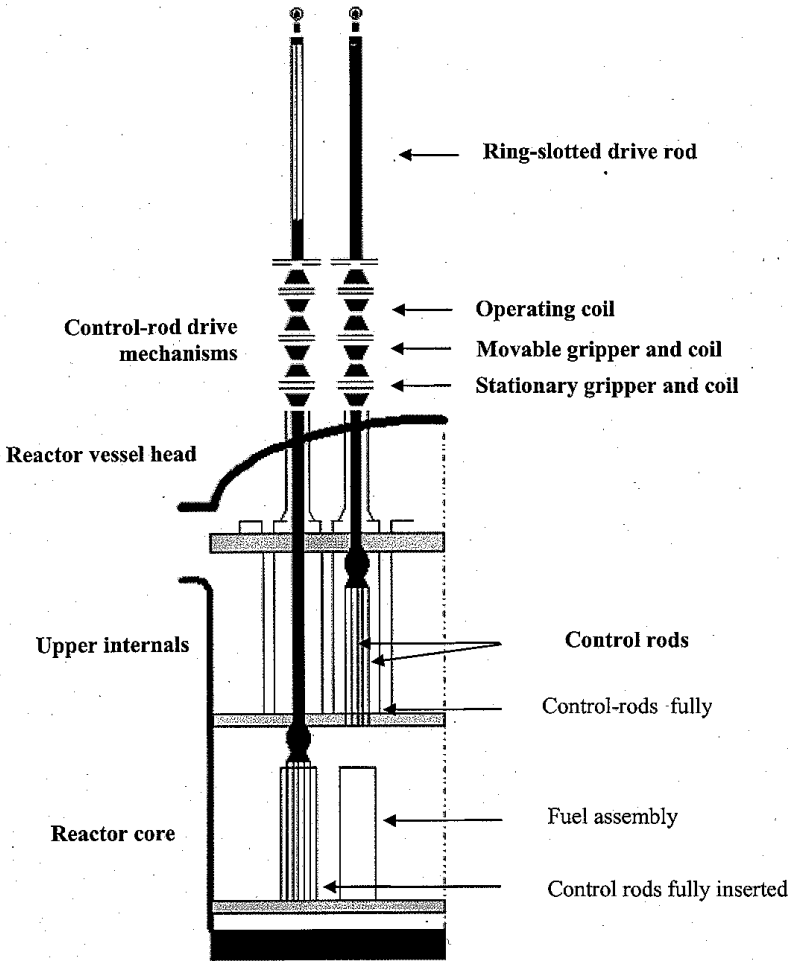


Figure 8. **View of PWR Rod Drives and Control Rods**



Appendix 2.

BWR Schemas

Figure 9. **View of a BWR Control Rod Drive**

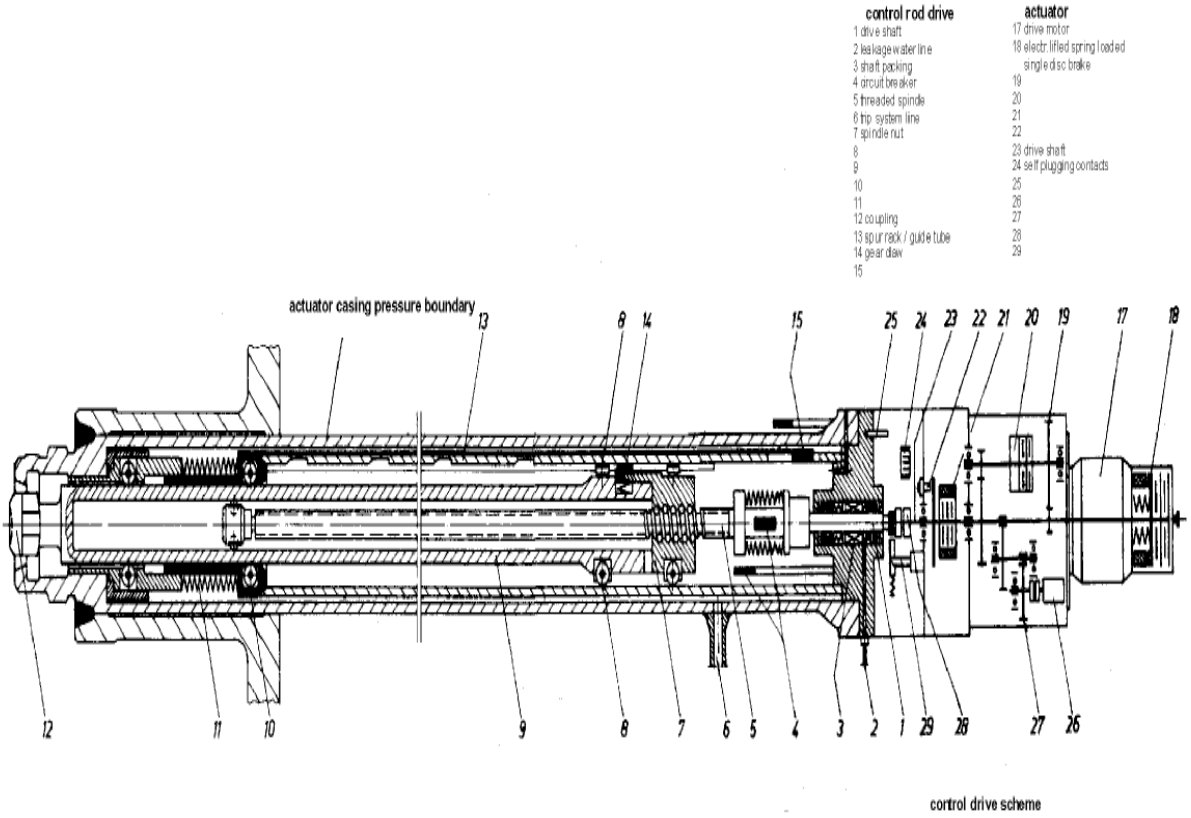


Figure 10. **Hydraulic Part of a German BWR Reactor Scram System**

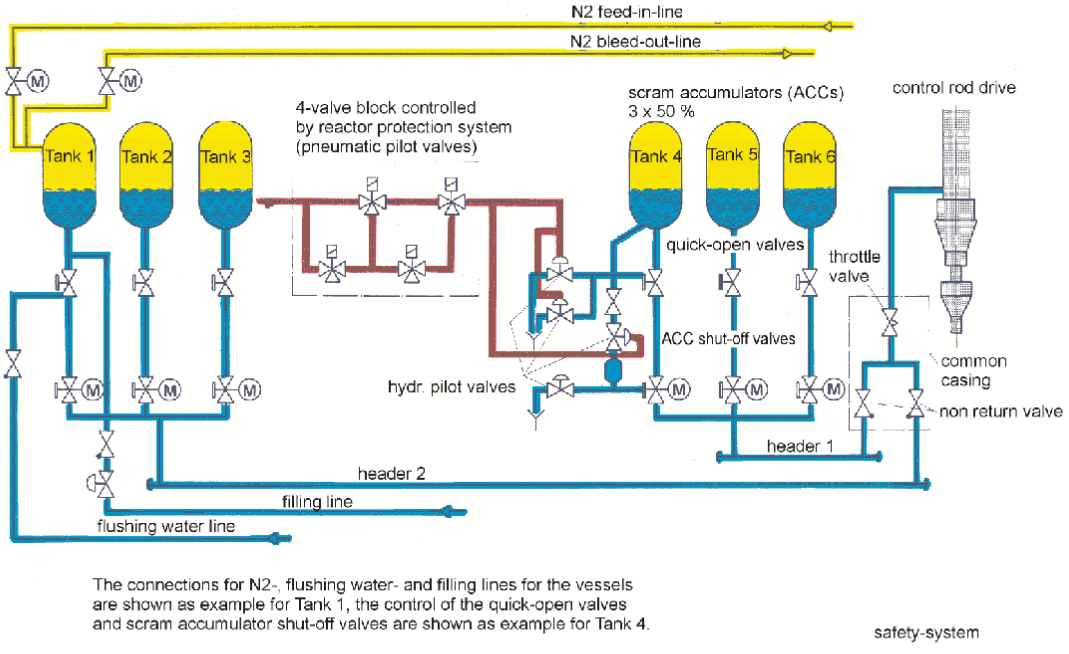


Figure 11. **Schematic Diagram of the Control Rod and Drive Assembly in Olkiluoto 1 and 2**

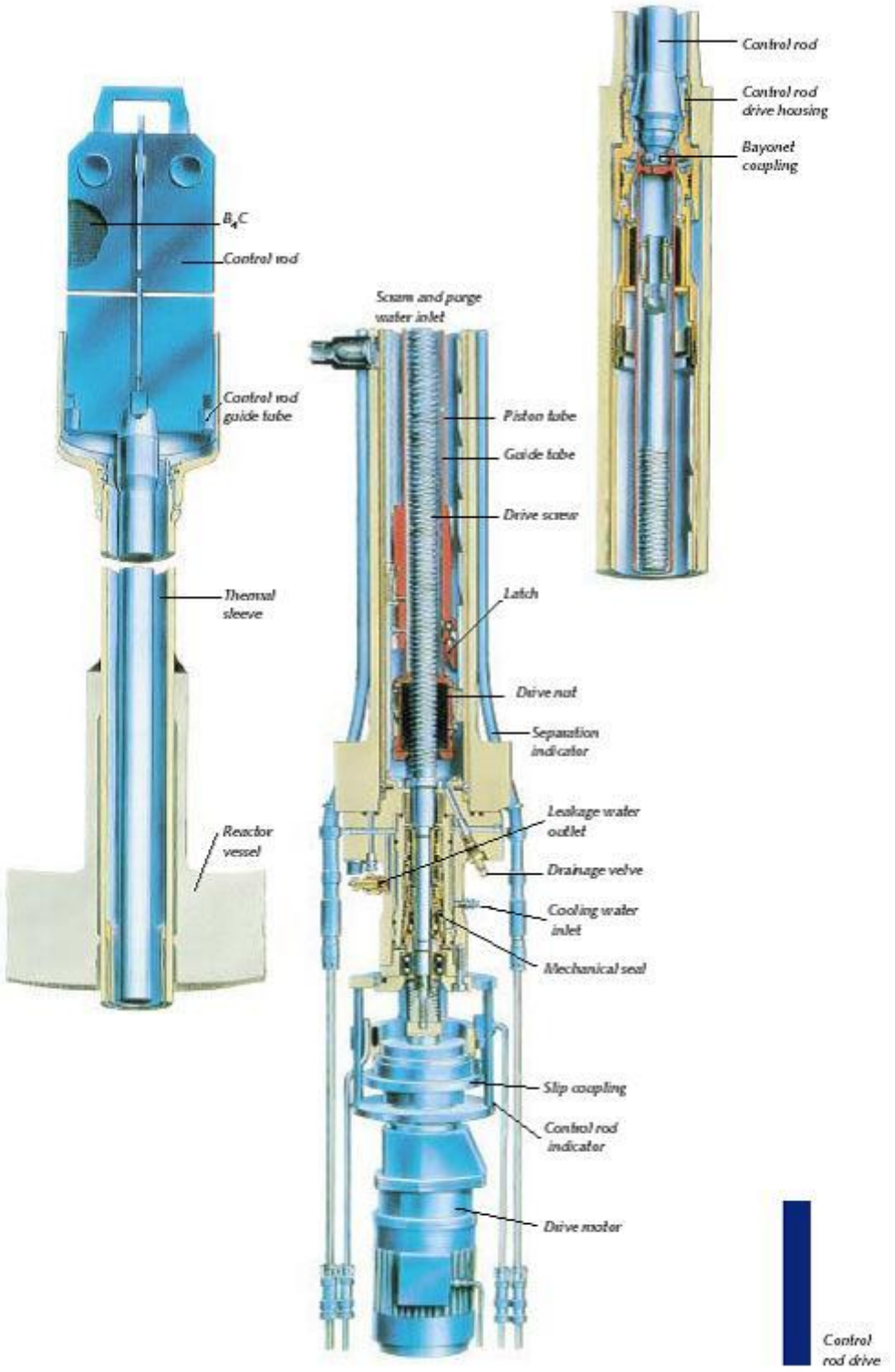


Figure 12. **Component boundary definition of the Control Rod and Drive Assembly as used in the Nordic component data collection [T Book]**

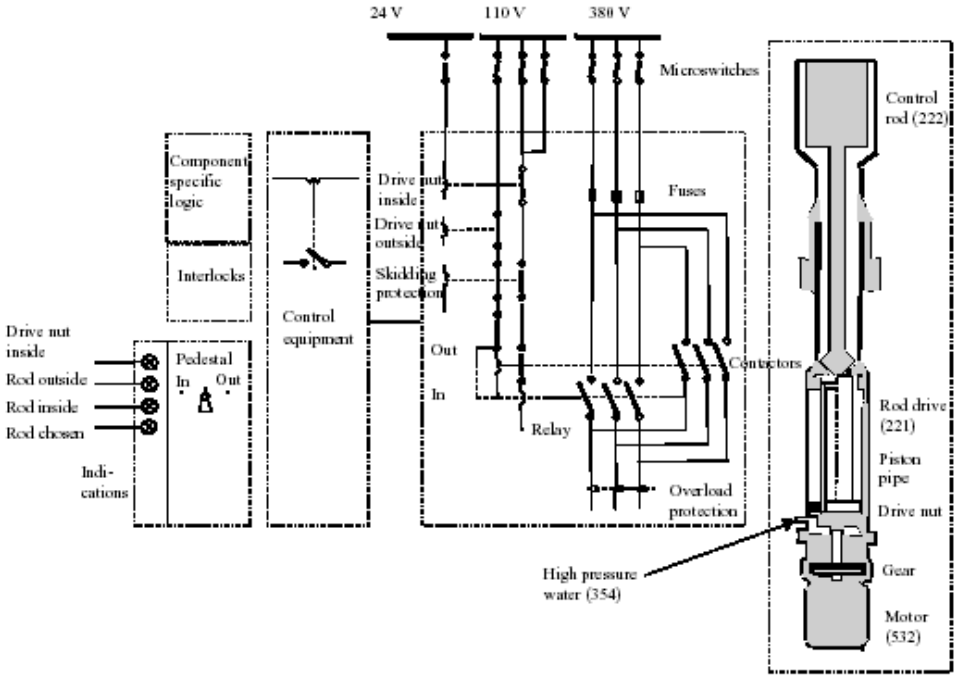
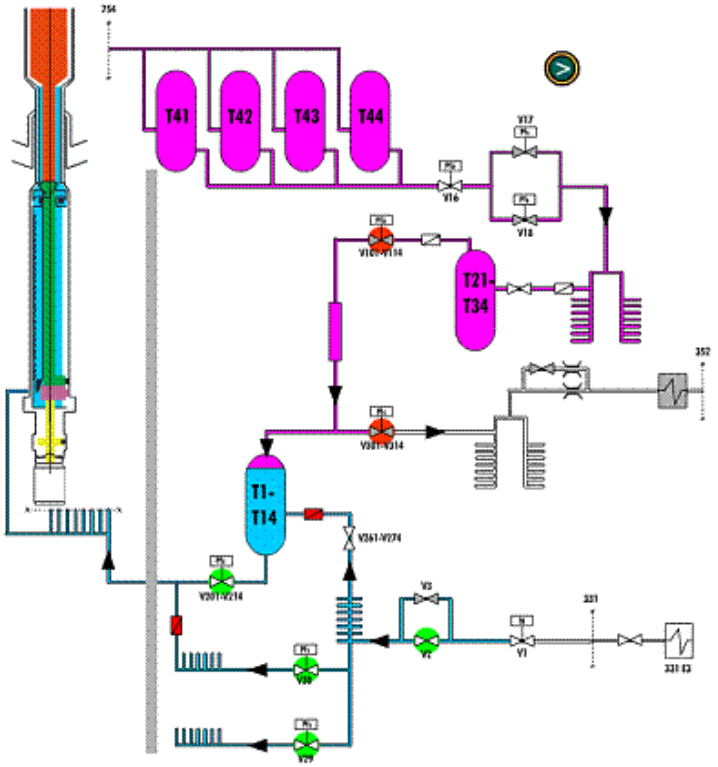


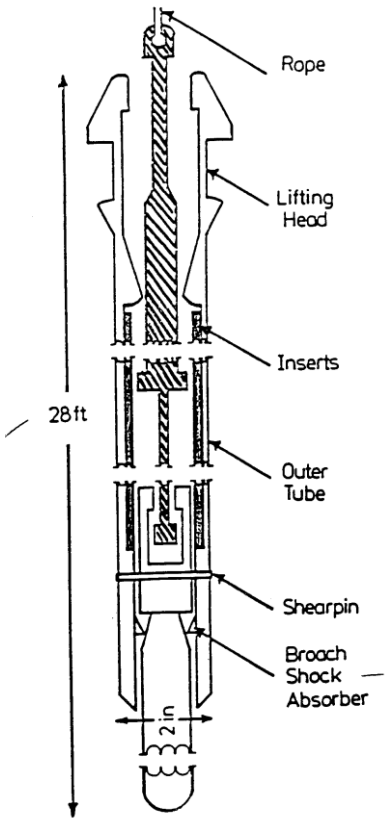
Figure 13. **Simplified process diagram for a train of Hydraulic Scram System in Olkiluoto 1 and 2. Internal isolation valve (non-return valve) and manual closing valves (used in maintenance) are omitted in this schematic picture.**



Appendix 3.

Magnox Schema

Figure 14. **Control Rod Schematic (Magnox)**



Appendix 4.

AGR Schema

Figure 15. **Control Rod Assembly (AGR)**