Unclassified **NEA/CSNI/R(99)14/REV1**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 18-Feb-2000
Dist. : 23-Feb-2000

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(99)14/REV1
Unclassified

COMPUTER-BASED SYSTEMS IMPORTANT TO SAFETY (COMPSIS)

REPORTING GUIDELINES

JULY 1999

English text only

87408

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

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

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

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

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of all OECD Member countries except New Zealand and Poland. The Commission of the European Communities takes part in the work of the Agency.

The primary objective of the NEA is to promote co-operation among the governments of its participating countries in furthering the development of nuclear power as a safe, environmentally acceptable and economic energy source.

This is achieved by:

- *encouraging harmonization of national regulatory policies and practices, with particular reference to the safety of nuclear installations, protection of man against ionising radiation and preservation of the environment, radioactive waste management, and nuclear third party liability and insurance;*
- *assessing the contribution of nuclear power to the overall energy supply by keeping under review the technical and economic aspects of nuclear power growth and forecasting demand and supply for the different phases of the nuclear fuel cycle;*
- *developing exchanges of scientific and technical information particularly through participation in common services;*
- *setting up international research and development programmes and joint undertakings.*

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

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

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

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

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

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

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

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

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

TABLE OF CONTENTS

1. INTRODUCTION

The objective of this procedure is to help the user to prepare an COMPSIS report on an event so that important lessons learned are most efficiently transferred to the database. This procedure focuses on the content of the information to be provided in the report rather than on its format.

The established procedure follows to large extend the procedure chosen by the IRS incident reporting system. However this database is built for I&C equipment with the purpose of the event report database to collect and disseminate information on events of significance involving Computer-Based Systems important to safety in nuclear power plants, and feedback conclusions and lessons learnt from such events.

For events where human performance is dominant to draw lessons, more detailed guidance on the specific information that should be supplied is spelled out in the present procedure. This guidance differs somewhat from that for the provision of technical information, and takes into account that the engineering world is usually less familiar with human behavioural analysis than with technical analysis.

2. EVENT SELECTION FOR REPORTING

The events to be reported to the COMPSIS database should be based on the national reporting criteria in the participating member countries. The aim is that all reports including computer based systems that meet each country reporting criteria should be reported. The database should give a broad picture of events/incidents occurring in operation with computer control systems.

3. MESSAGE TO BE CONVEYED

As soon as an event has been identified, the insights and lessons learnt to be conveyed to the international nuclear community shall be clearly identified.

4. TYPE OF REPORT

Only one type of report exists. Because of the specific nature of this database the reporting is based on the national documents (LERs) and other available documents.

5. REPORT CONTENT

5.1 Identification of the Necessary Information

From the available national documents on the event, extract and sort the following items (if available): the framework for coding is the IRS Coding. Reformatting of the codes are detailed within this report. The COMPSIS Coding, Appendix A, is to a large extend similar to the IRS but with some changes in Section 5: Cause of events.

A. General data, such as plant name/unit and date/time of the event.

B. Plant conditions before the event and methods of event discovery (in case of a deficiency).

C. The factual event sequence as observed, possibly including the observed degradations or malfunctions of systems and on line reasoning or reaction of people, with their impact on the event sequence. Identify clearly the observed cause/consequence relationships.

D. A consequence analysis, in order to determine whether or not some aspects of the event are indicators of indirect problems which could lead to a safety significant or a serious accident.

E. A safety analysis of the event, identifying all the observed and root deficiencies, as well as the investigation and corrective actions taken.

F. The causes and corrective actions should address technical as well as human aspects; an indication of how each given deficiency has been corrected is advisable.

G. Assessment by the regulatory body, to the extent possible.

H. If the event description and/or analysis require some knowledge unfamiliar to international readers in order to provide a good understanding, collect the necessary information on plant features.

5.2 Formalization of the Collected Information into the Report

In order to follow the recommended general format for COMPSIS reports, the following process should be applied.

On the basis of the description of the event (section 5.2.1) the event shall be analyzed in detail under the aspect of direct and potential impact to plant safety functions. The first part should show the common involvement of operation and safety systems (detailed proceeding see guidelines for the IRS Database) and the second part should show the special aspects of I&C functions, hardware and software. Keypoints should be:

- I&C functions
  - identification and description of the involved I&C functions

- I&C hardware
  - identification and description of the hardware malfunctions
  - identification of the failed hardware systems, components, modules
  - hardware redundancy and it' s part in the event proceeding

- I&C software
  - identification and description of software malfunctions
  - identification of the failed software

  - Off-line Software:
    Software for engineering, configuration, and maintenance (e.g. engineering tools, code generator, compiler, linker, locator)

  - On-line Software:
    Software that is running on the computer modules of the system

  - System software:
    (e.g. runtime environment, function block libraries, operating system, communication software, software for self monitoring, start-up, maintenance and troubleshooting)

  - Application software:
    (e.g. function diagram modules).

- I&C handling
  - identification and description of malfunctions due to human interaction
  - (e.g. periodic test, maintenance, etc.)

- I&C configuration management
  - eg., bad procedures, bad manuals for software modification

The schemes given in figures 1 and 2 show the dependencies.

In order to clarify the type of instrumentation and control failures to be included in the database the following definitions are given:

In IEC 61513 a computer-based system is defined as "I&C system whose functions are mostly dependent on, or completely performed by, using microprocessors, programmed electronic equipment or computers".

Definitions (IEEE Standard 610.12 - 1990, IEEE Standard Glossary of Software Engineering Terminology).

Fault	(1) A defect in a hardware device or component; for example, a short circuit or broken wire. (2) An incorrect step, process, or data definition in a computer program
Error	The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. for example, a difference of 30 meters between a computed result and the correct result.
Failure	The inability of a system or component to perform its required functions within specified performance requirements.
Mistake	A human action that produces an incorrect result (see Code 5.1.10.2)

Note: The fault tolerance discipline distinguishes between the human action (a mistake), its manifestation (a hardware or software fault), the result of the fault (a failure) and the amount by which the result is incorrect (the error).)

The following codes provide for indication of the type of fault or failure related specifically to computer-based I&C systems.

Computer Hardware Deficiency could be classified as follows:

Hardware is defined as the physical equipment used to process, store, or transmit computer programs or data. Hardware and software faults can be classified by persistence and by the source of the fault. Any fault falls into one of four persistence classes: (1) system requirements fault, (2) design fault, (3) permanent or operational fault, (4) transient fault. For example, a computer system is constructed according to some system requirements specification and corresponding hardware and software requirements specifications. If the computer system fails to perform as expected, but performs according to the system requirements, then the requirements specification is wrong. This is a system requirements fault. If the system fails, but still performs according to the hardware and software specifications, then the fault is in the specifications. This is a design fault. If, however, the system fails and does not meet either

the hardware or software specification, then the underlying fault is a permanent or operational fault. An example would be a broken wire. If the specifications are correct, but the system fails momentarily and then recovers on its own, the fault is a transient fault.

The hardware fault could also fall into one of three source classes: (1) environmental fault (see Code 5.1.6), (2) human fault (see Code 5.1.10), (3) unknown fault.

The types of hardware failures based on the failure modes are: (1) complete failure, and (2) partial failure.

Computer Software Deficiency could be classified as follows:

Software is defined as computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system. Software faults can be also classified by persistence and by the source of the fault. Any fault falls into one of three persistence classes: (1) design fault, (2) permanent or operational fault, (3) transient fault.

The computer software fault could also fall into one of several source classes; all considered here as software design faults. Examples are: (1) logic faults, (2) interface faults, (3) data definition faults, (4) database faults, (5) input/output faults, (6) computational faults, (7) data handling faults, (8) miscellaneous faults. An unknown fault would also be considered as a source class.

The types of software failures based on the failure modes are: (1) complete failure, and (2) partial failure.

5.2.1 Prepare the narrative description

Plant Features

Provide the technical and organizational data necessary to understand the event. Reactor systems and terminology are not universal. It may be helpful for other IRS users to include a brief description of the systems, practices, procedures and/or organizational characteristics that influenced the incident, especially if these are known to be peculiar to the plant or country. For a better understanding, descriptive names for equipment should be used rather than internal identification codes.

It is important to look at the details in Section 5.2 for the narrative description of the event for COMPSIS.

Event sequence and personnel reactions

All relevant information on what happened during the event and on the general context of the event. The following should be provided:

A. Situational aspects

(a) Plant conditions prior to the event.
(b) Operating modes or testing conditions.
(c) Equipment status.

B. Chronological information

(a) Chronological information indicating relevant time-scales.

(b) Identification of failures and successes in technical behaviour, up to and including during the recovery actions (Appendix A, Section 9).
For events where human aspects play a significant role, the following information should be provided where available:

(c) Identification of failures and successes in human behaviour, up to and including the recovery actions (Appendix A, Section 9).
Information on the nature and timing of recovery actions may provide additional insight into the complexity of the situation and the difficulties for the operators to detect and diagnose the problem at hand. Lessons may also be learned from the positive role of the plant personnel involved in the event.
If relevant, include a discussion of the recovery actions, providing information on how and when the recovery was achieved. Identify the persons involved in the recovery actions.

(d) Detection and diagnosis activities.
More specific information on the time delay needed for the detection of the human deficiencies and system failures, and for the diagnosis of the safety problem. Indicate, if applicable, any factor leading to a lengthy delay before a problem was detected or diagnosed.

(e) Human actions.

(f) Intra- and extra-team communication aspects.

This description should not focus too much on causes, in order not to duplicate the cause analysis.

Previously related events or precursors should be indicated.

If available, add figures, including layouts, photographs and/or drawings, in order to allow a better understanding of the environment in which the event occurred.

5.2.2 Prepare the safety assessment

Address here the actual and potential consequences of the observed problems. In particular, a discussion of the barriers which were broken by the observed deficiencies and the effective barrier that terminated the event should be included.

Special for the COMPSIS, the safety significance shall be discussed on the basis of actual and potential consequences of the analyzed events. Potential consequences by other known or possible boundaries of hardware or software architecture should be taken in consideration. (Level of details are given in Section 5.2).

When relevant, safety aspects related to human performance should be included.

If the assessments by the licensee and by the Regulatory body are different, this should be indicated.

5.2.3 Prepare the cause analysis section

Indicate clearly here, when relevant, the “direct or observed causes” as well as the “root causes”.

How did it happen?

The presentation and discussion of the "direct or observed causes” (i.e. the failures, actions, omissions or conditions which immediately produced the event) should answer the question "how did it happen?", identifying the technical or human deficiencies. It should give, to the extent possible, the results of the analysis identifying the failure mode including the nature of failures or errors *(Appendix A, Section 8).*

For events where human aspects play a significant role, the following information should be provided where available: include the type of observed human errors (*Appendix A, Section 5.1.10*) which contributed to the initiation of the event or affected in a direct way the operator or system response to the event.

The report should also provide the identified “ causal factors” relevant to the message to be conveyed. These causal factors are causes that, if corrected, would not by themselves have prevented the event, but are important enough to implement worthwhile corrective actions in order to improve the quality of the process or product.

Why did it happen?

A presentation and discussion of "root causes" should follow. These causes are fundamental causes that, if corrected, should prevent recurrence of the event or of its adverse environment. Both causal factors and root causes provide the answers to the question "why did it happen?".

For events where human aspects play a significant role, the following information should be provided where available: the human performance related causal factors and root causes (*Appendix A, Sections 5.5 and 5.6*).

If possible, make additional charts (include an event and causal factor chart) to illustrate the analysis results.

Are Common-cause aspects (CCF) involved?

If more than one I&C function hardware or software was involved the details should be outlined.

5.2.4 Prepare the lessons learned and corrective actions section

Describe the set of corrective actions taken by the utility to address the observed technical and human problems in the form of short term and long term actions. The priority of the various corrective measures should also be provided, if it emphasizes the significance of the various causes. They may cover administrative measures as well as hardware and software modifications taken to lower the likelihood of both technical and human failures.

This COMPSIS section will give general information on what was done to recover a functionally correct activity of the computer based system (short term corrective actions), on one hand, and on the other hand, what was decided to prevent falling in the same pit (long term corrective actions).

Information on the corrective actions should be provided with respect to the steps that have been followed from recovering of a correct activity of the computer-based system up to the final validation of the solution to solve the anomaly.

Usually, a first set of corrective actions are decided after discrepancies regarding the specified behaviour of the computer based system have lead to identify the anomalies and their first causes (i.e. the first layer of the source of the anomaly).

Other corrective actions could later on be decided as the root cause analysis, which currently needs months to be done, shows necessary changes in maintenance or design of the computer based system.

Example of corrective actions:

It is necessary to distinguish between recovery actions that are taken to bypass the anomaly from those actions that are undertaken to solve the anomaly. Corrective actions are of the second category.

Short term corrective actions types:

- changes in operational procedures to operate the computer based system,
- functional tests on the computer based system to validate that changes.

Long term corrective actions types:

- changes in maintenance or design to solve the anomaly,
- validation of the new solution on premises,
- validation of the new configuration of the computer based system on site

For events where human aspects play a significant role, include when available:

(a) Changes in attitudes or habits of persons or groups
(b) Changes to training; indicate what was lacking in terms of knowledge and know-how
(c) Changes to procedures
(d) Organizational changes
(e) Improvement in ergonomics
(f) Hardware modifications which influence man-machine interaction.
(g) Software modifications which influence man-machine interaction.

Describe also any specific actions taken by the Regulatory Body in response to the event.

Indication of the generic character of the actions taken or of difficulties in designing or implementing the corrective actions may be useful.

The content and formulation of the lessons (cause analysis, corrective actions) should be practical and understandable (applicable) to other NPPs, in accordance with the message to be conveyed.

5.2.5 Prepare the abstract

The objective of the abstract is to convey the main messages contained in the report, essential for the understanding of the relevance of the event or conditions. A good abstract should give, in a concise form (maximum 25 lines), a brief description of the event, its safety relevance, its causes, the lessons learned and the corrective actions taken.

5.2.6 Choose a title

The title should be a very short characterization of the event, emphasizing its most significant features.

5.2.7 Prepare the cover page and codes

5.2.7.1 Cover page

Fill in the cover page information to identify the event.

Title
Fill in the title as determined in Section 5.2.6.

Plant Name and code
The standard plant name and unit number shall be indicated.

Date of incident
The Date of Incident should be in the form YYYY/MM/DD if a specific date can be defined.

5.2.7.2 Codes

As the codes are provided for retrieval purposes, they must reflect the event conditions, the observed phenomena and the problems encountered.

More than one code can be selected under each category. Naturally, the more detailed the code, the better. However, if a detailed code is selected, its parent codes should not be selected.

Refer to *Appendix A,* Sections 1 to 9 for the definitions and usage of the available codes.

For events where human aspects play a significant role, the following information should be provided where available:

(a) Plant staff involvement (*Appendix A, Section 5.3*).
(b) Type of activity at the time of the event (*Appendix A, Sections 5.5.1 and 5.5.2*).
(c) Characterization of the personnel work practices (*Appendix A, Section 5.7.2*).
(d) Characterization of the working conditions (*Appendix A, Sections 5.5.4 and 5.5.5*).
(e) All other related organizational aspects (*Appendix A, Sections 5.5.3 to 5.5.9*).

APPENDIX A

COMPSIS Coding:
Based on IRS Coding changed to COMPSIS specific codes in Section 5: Cause of Event

DICTIONARY OF CODES

REACTOR TYPES

BWR	Boiling Water Reactor
FBR	Fast Breeder Reactor
GCR	Gas Cooled Reactor (graphite or heavy water moderated; includes AGR, HTGR and HWGCR)
GEN	Generic report (reactor type is irrelevant)
HWLWR	Heavy Water moderated, boiling Light Water cooled Reactor
LWGR	Light Water cooled, Graphite moderated Reactor (e.g. RBMK)
PHWR	Heavy Water moderated, Pressure tube Reactor
PWR	Pressurized Water Reactor (includes WWER)
SGHWR	Steam Generating Heavy Water Reactor

COUNTRY CODES

AM	Armenia
AR	Argentina
AT	Austria
BE	Belgium
BG	Bulgaria
BR	Brazil
CA	Canada
CH	Switzerland
CN	China
CS	Former Czechoslovakia
CU	Cuba
CZ	Czech Republic
DE	Germany
EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
HU	Hungary
IL	Israel
IN	India
IQ	Iraq
IR	Iran
IT	Italy
JP	Japan
KR	Republic of Korea
LT	Lithuania
LY	Libya
MX	Mexico
NL	Netherlands
PH	Philippines
PK	Pakistan
PL	Poland
RO	Romania
RU	Russian Federation
SE	Sweden
SL	Slovenia
SK	Slovakia
TH	Thailand
TR	Turkey
UA	Ukraine
US	United States of America
YU	Yugoslavia
ZA	South Africa

1. REPORTING CATEGORIES

1.1 Unanticipated releases of radioactive material or exposure to radiation

1.1.1 Unanticipated releases of radioactive material
1.1.2 Exposure to radiation that exceeds prescribed dose limits for members of the public
1.1.3 Unanticipated exposure to radiation for site personnel

1.2 Degradation of barriers and safety related systems

1.2.1 Fuel cladding failure
1.2.2 Degradation of primary coolant pressure boundary, main steam or feedwater line
1.2.3 Degradation of containment function or integrity
1.2.4 Degradation of systems required to control reactivity
1.2.5 Degradation of systems required to assure primary coolant inventory and core cooling
1.2.6 Degradation of essential support systems

1.3 Deficiencies in design, construction, operation (including maintenance and surveillance), quality assurance or safety evaluation

1.3.1 Deficiencies in design
1.3.2 Deficiencies in construction
1.3.3 Deficiencies in operation (including maintenance and surveillance)
1.3.4 Deficiencies in quality assurance
1.3.5 Deficiencies in safety evaluation

1.4 Generic problems of safety interest

1.5 Consequential actions

1.6 Events of potential safety significance

1.7 Effects of unusual external events of either man-made or natural origin

1.8 Categories of other nature

2. PLANT STATUS PRIOR TO THE EVENT

2.0 Not applicable

2.1 On power

2.1.1 Full allowable power
2.1.2 Reduced power (including zero power)
2.1.3 Raising power or starting up
2.1.4 Reducing power
2.1.5 Refueling on power

2.2 Hot shutdown (reactor sub-critical)

2.2.1 Hot standby (coolant at normal operating temperature)
2.2.2 Hot shutdown (coolant below normal operating temperature)

2.3 Cold shutdown (reactor sub-critical and coolant temperature < 93°C)

2.3.1 Cold shutdown with closed reactor vessel
2.3.2 Refueling or open vessel (for maintenance)
2.3.2.1 Refueling or open vessel – all or some fuel inside the core
2.3.2.2 Refueling or open vessel – all fuel out of the core
2.3.3 Mid-loop operation (PWR)

2.4 Pre-operational

2.4.1 Construction
2.4.2 Commissioning

2.5 Testing or maintenance was being performed

2.6 Decommissioning

3. FAILED/AFFECTED SYSTEMS

3.A Primary reactor systems

3.AA Reactor core (fuel assemblies, control and poison rods, guide thimbles, ...)
3.AB Control rod drive (mechanism, motor, power supply, hydraulic system, other shutdown systems)
3.AC Reactor vessel (with core internals, PHWR or LWGR pressure tubes, ...)
3.AD Moderator and auxiliaries (PHWR, ...)
3.AE Primary coolant (pumps and associated materials, loop piping, ...)
3.AF Pressure control (includes primary safety relief valves)
3.AG Recirculating water (BWR, ...)
3.AH Steam generator, boiler, steam drum
3.AK At power fuel handling systems (PHWR, LWGR, GCR)
3.AL Annulus gas (PHWR, LWGR)

3.B Essential reactor auxiliary systems

3.BA Reactor core isolation cooling (BWR)
3.BB Auxiliary and emergency feedwater
3.BC Emergency poisoning function (PWR mainly with the boron injection tank, chemical and volume control system participation)
3.BD Standby liquid control (BWR)
3.BE Residual heat removal (PWR and BWR except emergency core cooling functions)
3.BF Chemical and volume control (PWR with main pumps seal water, ...)
3.BG Emergency core cooling (core spray or relevant parts of residual heat removal, chemical and volume control system)
3.BH Main steam pressure relief (reactors which have secondary loops)
3.BK Nuclear boiler overpressure protection (BWR)
3.BL Core flooding accumulator (PWR)
3.BP Failed fuel detection (GCR)
3.BQ Gas cleanup system (LWGR, PHWR)

3.C Essential service systems

3.CA Component cooling water (including reactor building closed cooling water)
3.CB Essential raw cooling or service water
3.CC Essential compressed air
3.CD Borated or refueling water storage (PWR)
3.CE Condensate storage
3.CF CO2 injection and storage (GCR)

3.D Essential auxiliary systems

3.DA Spent fuel pool or refueling pool cooling and cleanup
3.DB Containment isolation (with BWR leakage control and air lock door seals)
3.DC Main steam or feedwater isolation function (with BWR main steam isolation valve leakage control)
3.DD Containment spray and ice condensers
3.DE Containment pressure suppression (not including spray)
3.DF Containment combustible gas control
3.DG Essential auxiliary steam (GCR)

3.E Electrical systems

3.EA High voltage AC (greater than 15kV including off-site power)
3.EB Medium voltage AC (600V to 15kV)
3.EC Low voltage AC (less than 600V – mainly 480V)
3.ED Vital instrumentation AC and control AC
3.EE DC power
3.EF Emergency power generation and auxiliaries (includes fuel oil supply)
3.EG Security and access control
3.EH Communication and alarm annunciation

3.F Feedwater, steam and power conversion systems

3.FA Main steam and auxiliaries (including auxiliary steam)
3.FB Turbogenerator and auxiliaries
3.FC Main condenser and auxiliaries (non-condensable gases extraction and treatment)
3.FE Turbine by-pass
3.FG Condensate and feedwater
3.FM Condensate demineralizer
3.FN Circulating or condenser cooling water (including raw cooling and service water)

3.H Heating, ventilation and air conditioning systems (HVAC)

3.HA Primary reactor containment building HVAC
3.HB Primary containment vacuum and pressure relief
3.HC Secondary containment recirculation, exhaust and gas treatment
3.HD Drywell or wetwell HVAC and purge and inerting (BWR)
3.HE Reactor or nuclear auxiliary building HVAC
3.HF Control building HVAC (including main control room HVAC)
3.HG Fuel building HVAC
3.HH Turbine building HVAC
3.HK Waste management building HVAC
3.HM Miscellaneous structures HVAC
3.HN Chilled water
3.HP Plant stack
3.HQ Emergency generator building HVAC
3.HR Seismic/Bunkered emergency control building HVAC

3.I Instrumentation and control systems

3.IA Plant/Process computer (including main and auxiliary computers)
3.IB Fire detection
3.IC Environment monitoring
3.ID Turbogenerator instrumentation and control
3.IE Plant monitoring (including the main control room equipment and various remote control functions)
3.IF In-core and ex-core neutron monitoring
3.IG Leak monitoring
3.IH Radiation monitoring (in the plant and of workers)
3.IK Reactor power control
3.IL Recirculation flow control (BWR)
3.IM Feedwater control
3.IN Reactor protection
3.IP Engineered safety features actuation (including emergency systems actuation)
3.IQ Non-nuclear instrumentation

3.K Service auxiliary systems

3.KB Sampling
3.KC Control and service air (non-essential) and compressed gas
3.KD Demineralized water
3.KE Material and equipment handling
3.KG Nuclear fuel handling and storage
3.KH Fire protection
3.KP Chemical additive injection

3.S Structural systems

3.SA Primary reactor containment building
3.SB Secondary reactor containment building or vacuum building (PHWR)
3.SC Reactor or nuclear auxiliary building
3.SD Control building
3.SE Emergency generator building
3.SF Fuel building (including wet and dry storage buildings)
3.SG Turbine building
3.SH Waste management building
3.SK Pumping stations
3.SL Backup ultimate heat sink building
3.SM Cooling towers
3.SN Switchyard (enclosed/open)
3.SP Seismic/bunkered emergency control building

3.W Waste management systems

3.WA Liquid radwaste
3.WB Solid radwaste
3.WC Gaseous radwaste
3.WD Non-radioactive waste (liquid, solid and gaseous)
3.WE Steam generator blowdown
3.WF Plant drainage (floor, roof, ...)
3.WG Equipment drainage (including vents)
3.WH Suppression pool cleanup (BWR)
3.WK Reactor water cleanup (BWR, PHWR, LWGR,...)

3.Z None of the above systems

4. FAILED/AFFECTED COMPONENTS

4.0 No specific component involved

4.1 Instrumentation (gauges, transmitters, sensors)

4.1.0 Other
4.1.1 Pressure
4.1.2 Temperature
4.1.3 Level
4.1.4 Flow
4.1.5 Radiation/Contamination
4.1.6 Concentration
4.1.7 Position
4.1.8 Dewpoint, moisture
4.1.9 Neutron flux (detectors, ion chambers and associated components)
4.1.10 Speed measuring
4.1.11 Fire detectors
4.1.12 Hydrogen detectors
4.1.13 Electrical (current, voltage, power, ...)

4.2 Mechanical

4.2.0 Other
4.2.1 Pumps, compressors, fans
4.2.2 Turbines (steam, gas, hydro), engines (diesel, gasoline, ...)
4.2.3 Valves (including safety/relief/check/solenoid valves), valve operators, controllers, dampers and fire breakers, seals and packing
4.2.4 Heat exchangers (heaters, coolers, condensers, boilers, air dryer, ...), heat exchanger tube plugs
4.2.5 Tanks, pressure vessels (e.g. reactor vessel and internals, accumulators)
4.2.6 Tubes, pipes, ducts
4.2.7 Fittings, couplings (including transmissions and gear boxes), hangers, supports, bearings, thermal sleeves, snubbers
4.2.8 Strainers, screens, filters, ion exchange columns
4.2.9 Penetration (personnel access, equipment access, fuel handling, ...)
4.2.10 Control or protective rods and associated components or mechanisms, fuel elements
4.2.11 Fuel storage racks, fuel storage casks and fuel transport containers

4.3 Electrical

4.3.0 Other
4.3.1 Switchyard equipment (switchgear, transformers, buses, line isolators, ...)
4.3.2 Circuit breakers, power breakers, fuses
4.3.3 Alarms
4.3.4 Motors (for pumps, fans, compressors, valves, motor generators, ...)
4.3.5 Generators of emergency and stand-by power
4.3.6 Main generator and auxiliaries
4.3.7 Relays, connectors, hand switches, push buttons, contacts
4.3.8 Wiring, logic circuitry, controllers, starters, electrical cables

4.4 Computers

4.4.1 Computer hardware
4.4.2 Computer software

5. CAUSE OF THE EVENT

5.1 Cause

5.1.0 Unknown or other

5.1.1 Mechanical failure

5.1.1.0 Other mechanical failure
5.1.1.1 Corrosion, erosion, fouling
5.1.1.2 Wear, fretting, lubrication problem
5.1.1.3 Fatigue
5.1.1.4 Overloading (including mechanical stress and overspeed)
5.1.1.5 Vibration
5.1.1.6 Leak
5.1.1.7 Break, rupture, crack, weld failure
5.1.1.8 Blockage, restriction, obstruction, binding, foreign material
5.1.1.9 Deformation, distortion, displacement, spurious movement, loosening, loose parts

5.1.2 Electrical failure

5.1.2.0 Other electrical failure
5.1.2.1 Short-circuit, arcing
5.1.2.2 Overheating
5.1.2.3 Overvoltage
5.1.2.4 Bad contact, disconnection
5.1.2.5 Circuit failure, open circuit
5.1.2.6 Ground fault
5.1.2.7 Undervoltage, voltage breakdown
5.1.2.8 Faulty insulation
5.1.2.9 Failure to change state

5.1.3 Chemical or core physics failure

5.1.3.0 Other chemical or core physics failure
5.1.3.1 Chemical contamination, deposition
5.1.3.2 Uncontrolled chemical reaction
5.1.3.3 Core physics problems
5.1.3.4 Poor chemistry or inadequate chemical control

5.1.4 Hydraulic/pneumatic failure

5.1.4.0 Other hydraulic/pneumatic failure
5.1.4.1 Water hammer, abnormal pressure, pressure fluctuations, over pressure
5.1.4.2 Loss of fluid flow
5.1.4.3 Loss of pressure
5.1.4.4 Cavitation
5.1.4.5 Gas binding
5.1.4.6 Moisture in air systems
5.1.4.7 Vibration due to fluid flow

5.1.5 Instrumentation and control failure

5.1.5.0 Other instrumentation and control failure
5.1.5.2 False response, loss of signal, spurious signal
5.1.5.3 Oscillation
5.1.5.4 Set point drift, parameter drift
5.1.5.5 Computer hardware deficiency
5.1.5.5.1 Permanent or operational fault
A permanent fault is a fault where some portion of the computer system fails or degrades and must be repaired in order to return the system to a state that meets design specifications. Examples are electronic and mechanical faults.
5.1.5.5.2 Transient fault
A transient fault is a fault that can cause a computer system failure, but is no longer present when a system is restarted and cannot, generally, be duplicated. Frequently the root cause of a transient fault cannot be determined. Examples include power supply noise and timing errors. In some computer systems majority of all faults are transient.
5.1.5.5.3 Unknown fault
An unknown fault is a fault whose root cause was not yet identified. All such faults are also transient faults.
5.1.5.5.4 Latent/Hidden Fault (fault not self-signalled):
A latent hidden fault is a fault that has in the moment of occurrence no impact to the system functions or to monitoring devices. The faults are only detected by tests or demand.
5.1.5.5.5 Complete failure
A complete failure is a failure resulting in deviations in characteristics beyond specified limits such as to complete lack of the required function.
5.1.5.5.6 Partial failure
A partial failure is a failure resulting in deviations in characteristics beyond specified limits but not such as to cause complete lack of required function.

5.1.5.6 Computer software deficiency

5.1.5.6.1 Permanent or operational fault

A permanent fault is a fault where some portion of the computer system fails or degrades and must be repaired in order to return the system to a state that meets design specifications. Examples are database corruption and some human faults.

5.1.5.6.2 Transient fault

A transient fault is a fault that can cause a computer system failure, but is no longer present when a system is restarted and, generally, cannot be duplicated. Frequently the root cause of a transient fault cannot be determined.

5.1.5.6.3 Software design fault

A software design fault is a bug or an error in a program. It includes the following types of faults although some of them are not typical software faults:

- Logic faults
- Interface faults
- Data definition faults
- Database faults
- Input/output faults
- Computational faults
- Data handling faults
- Miscellaneous faults.

5.1.5.6.4 Unknown fault

An unknown fault is a fault whose root cause was not identified. All such faults are also transient faults.

5.1.5.6.5 Latent/hidden failure

Complete failure

A complete failure is a failure resulting in deviations in characteristics beyond specified limits such as to complete lack of the required function.

5.1.5.6.6 Partial failure

A partial failure is a failure resulting in deviations in characteristics beyond specified limits but not such as to cause complete lack of required function.

5.1.5.7 Computer system deficiency

5.1.5.7.1 System requirements fault

A system requirements fault is a fault that can be corrected by revising the systems requirements specification and the corresponding redesigning of the computer system. A system requirements fault can lead to failure of the computer system to perform as expected.

5.1.5.7.2 Design fault

A design fault is a fault that can be corrected by redesign. A design fault can lead to many failures before it is diagnosed and corrected.

5.1.6 Environmental (abnormal conditions inside plant)

An environmental fault is a fault that occurs due to conditions outside the computer system, but which affects the system. This can be duplicated by exposing the equipment, component, or system to the same environmental conditions as when the fault occurred. Faults due to high temperature, humidity, freezing, electrical surge are examples of environmental faults. Most of these faults are under IRS Code 5.1.6 (5.1.6.0 through 5.1.6.8) and 5.1.7. Faults due to electromagnetic/radio frequency interference (E.I./R.I.) and electrostatic discharge would fall in this section. Environmental faults could also fall under the design, operational or transient fault type above.

5.1.6.0 Other internal environmental cause
5.1.6.1 High temperature
5.1.6.2 Pressure
5.1.6.3 Humidity
5.1.6.4 Flooding, water ingress
5.1.6.5 Low temperature, freezing
5.1.6.6 Radiation, contamination, irradiation of parts
5.1.6.7 Dropped loads, missiles, high energy impacts
5.1.6.8 Fire, burning, smoke, explosion
5.1.6.9 Electromagnetic interference (EMI)

5.1.7 Environmental (external to the plant)

An environmental fault is a fault that occurs due to conditions outside the computer system, but which affects the system. This can be duplicated by exposing the equipment, component, or system to the same environmental conditions as when the fault occurred. Faults due to high temperature, humidity, freezing, electrical surge are examples of environmental faults. Most of these faults are under IRS Code 5.1.6 (5.1.6.0 through 5.1.6.8) and 5.1.7. Faults due to electromagnetic/radio frequency interference (E.I./R.I.) and electrostatic discharge would fall in this section. Environmental faults could also fall under the design, operational or transient fault type above.

5.1.7.0 Other external environmental cause (fire, toxic/explosive gasses,...)
5.1.7.1 Lightning strikes
Electromagnetic Interference (EMI)
5.1.7.2 Flooding
5.1.7.3 Storm, wind loading
5.1.7.4 Earthquake
5.1.7.5 Freezing
5.1.7.6 High ambient temperature
5.1.7.7 Heavy rain or snow

5.1.10 Human factors
This code should be used for all human faults hardware or software in COMPSIS
5.1.10.1 Slip or lapse
5.1.10.2 Mistake
5.1.10.3 Violation
5.1.10.4 Sabotage

5.3 Inadequate human action – plant staff involved

5.3.1 Maintenance
5.3.2 Operations
5.3.3 Technical and engineering
5.3.4 Management and administration

5.4 Inadequate human action – type of activity

5.4.1 Not relevant
5.4.2 Normal operations
5.4.3 Shutdown operations
5.4.4 Equipment startup
5.4.5 Planned/preventive maintenance
5.4.6 Isolating/de-isolating
5.4.7 Repair (unplanned/breakdown maintenance)
5.4.8 Routine testing with existing procedures/documents
5.4.9 Special testing with one-off special procedure
5.4.10 Post-modification testing
5.4.11 Post-maintenance testing
5.4.12 Fault finding
5.4.13 Commissioning (of new equipment)
5.4.14 Recommissioning (of existing equipment)
5.4.15 Decommissioning
5.4.16 Fuel handling/refueling operations
5.4.17 Inspection
5.4.18 Abnormal operation (due to external or internal constraints)
5.4.19 Engineering review
5.4.20 Modification implementation
5.4.21 Training
5.4.22 Actions taken under emergency conditions
5.4.23 Other activity

5.5 Human performance related causal factors and root causes

5.5.1 Verbal communications
5.5.2 Personnel work practices
5.5.2.0 Others
5.5.2.1 Control of task/independent verification

5.5.2.2 Complacency/lack of motivation/inappropriate habits
5.5.2.3 Use of improper tools and equipment
5.5.3 Personnel work scheduling
5.5.4 Environmental conditions
5.5.5 Man-machine interface
5.5.6 Training/qualification
5.5.7 Written procedures and documents
5.5.8 Supervisory methods
5.5.9 Work organization
5.5.9.0 Others
5.5.9.1 Shift/team size or composition
5.5.9.2 Planning/preparation of work
5.5.10 Personal factors
5.5.10.0 Others
5.5.10.1 Fatigue
5.5.10.2 Stress/perceived lack of time/boredom
5.5.10.3 Skill of the craft less than adequate/not familiar with job performance standards

5.6 Management related causal factors and root causes

5.6.0 Others
5.6.1 Management direction
5.6.2 Communication or co-ordination
5.6.3 Management monitoring and assessment
5.6.4 Decision process
5.6.5 Allocation of resources
5.6.6 Change management
5.6.7 Organizational/safety culture
5.6.8 Management of contingencies

5.7 Equipment related causal factors and root causes

5.7.0 Others
5.7.1 Design configuration and analysis
5.7.2 Equipment specification, manufacture and construction
5.7.3 Maintenance, testing or surveillance

6. EFFECTS ON OPERATION

6.0 Unidentified or no significant effect on operation or not relevant

6.1 Reactor scram

6.1.1 Automatic reactor scram
6.1.2 Manual reactor scram

6.2 Controlled shutdown

6.3 Load reduction

6.3.1 Automatic load reduction
6.3.2 Manual load reduction

6.4 Activation of engineered safety features

6.5 Challenge to safety or relief valve

6.5.1 Challenge to safety or relief valve in the primary circuit
6.5.2 Challenge to safety or relief valve in the steam or condensate cycle

6.6 Unanticipated or significant release of radioactive materials

6.6.1 Unanticipated or significant release of radioactive materials outside the plant
6.6.2 Unanticipated or significant release of radioactive materials inside the plant

6.7 Unplanned or significant radiation exposure of personnel or public

6.8 Personnel or public injuries

6.9 Outage extension

6.10 Exceeding technical specification limits

7. CHARACTERISTICS OF THE INCIDENT

7.0 Other characteristics

7.1 Degraded fuel

7.2 Degraded reactor coolant boundary

7.3 Degraded reactor containment

7.4 Loss of safety function

7.5 Significant degradation of safety function

7.6 Failure or significant degradation of the reactivity control

7.7 Failure or significant degradation of plant control

7.8 Failure or significant degradation of heat removal capability

7.9 Loss of off-site power

7.10 Loss of on-site power

7.11 Transient

7.11.0 Other transient
7.11.1 Power transient
7.11.2 Temperature transient
7.11.3 Pressure transient
7.11.4 Flow transient

7.12 Physical hazards (internal or external to the plant)

7.13 Discovery of major condition not previously considered or analysed

7.14 Fuel handling incident

7.15 Radwaste incident

7.16 Security, safeguards, sabotage or tampering incident

8. NATURE OF FAILURE OR ERROR

8.0 Not relevant

8.1 Single failure or single error

8.2 Multiple failure or multiple error

8.2.1 Independent multiple failures or errors
8.2.2 Dependent multiple failures or errors
8.2.3 Recurrent failure or error

8.3 Common cause failure (including potential for CCF)

In COMPSIS events this code should be used if more than one function was involved. Even if only one hardware or software component is involved but the potential of dependent failure is present this code should be used.

8.4 Significant or unforeseen interaction between systems

9. NATURE OF RECOVERY ACTIONS

9.0 Not relevant

9.1 Recovery by human action

9.1.1 Recovery by foreseen human action
9.1.2 Recovery by unforeseen human action

9.2 Recovery by automatic plant action or by design

9.3 No recovery