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

Computer-based Systems Important to Safety (COMPSIS) Project: Second Period Operation (2008-2011)

Final Report

NUCLEAR ENERGY AGENCY

Unclassified **NEA/CSNI/R(2012)12**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **19-Jul-2012**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2012)12
Unclassified

Computer-Based Systems Important to Safety (COMPSIS) Project: Second Period Operation (2008-2011)

Final Report

This report is an update of report CSNI/R(2008)13

JT03324854

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'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.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

During the mid-1990s a Task group was formed within the Organisation for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA), to exchange information on events involving computer-based systems. In 2005 the OECD/NEA Steering Committee agreed to establish the international Computer-Based Systems Important to Safety (COMPSIS) project to encourage multilateral cooperation in the collection and analysis of data relating to computer-based system events in nuclear facilities. The main objective of the project was to improve the safety of nuclear facilities by utilising operating experience and providing common resources for the analytical framework of qualitative and quantitative assessments.

The analytical frame work has been the main focus of the first COMPSIS project period (2005–2007), with organisations from Finland, Germany, Hungary, Japan, the Republic of Korea, Slovak Republic, Sweden, Switzerland, the United States and Chinese Taipei who all have taken part in the project. The initial inputted event (total of twenty-two) has been limited as the steer group spent more effort working to perfect the COMPSIS web site coding guidelines as a function of this analytical frame work. This direction followed closely the first three of five objectives from the COMPSIS Project charter. This effort continued into the second COMPSIS project period (2008-2011) as countries became more familiar with the website's analytical protocol and maturing confidence with the coding guidelines, selected root causes and possible mitigation responses.

Though part of the original charter objectives were designed to decrease the uncertainty when recording research grade quality events, there exists the task on how to complete the last two charter objectives: developing defences against an event and a risk analysis of event attributes and dominant contributors. A key issue for the COMPSIS members was how to increase the number of events for processing. Without this increased number there was no way to begin to assess the coding guidance website or a real event analysis aspect of well-populated COMPSIS database. A key question while assuming that coding guidelines would maintain high level quality and consistency of input data is can the COMPSIS project continue to develop enough knowledge about the events so that an informed decision on software based I&C equipment can be made? An operating experience decision when using computers in a nuclear power plant that can be based upon a lesson learned from multiple of single events.

The purpose of this report is to determine whether the published events collected during the extended second period provides the opportunity for extracting lessons learned and improve the safety of nuclear facilities when modernizing with digital computer based equipment. Since all measurements are in error in some way or another, a method must be employed to determine viable lessons that can be used to develop defences against event occurrences /1/.

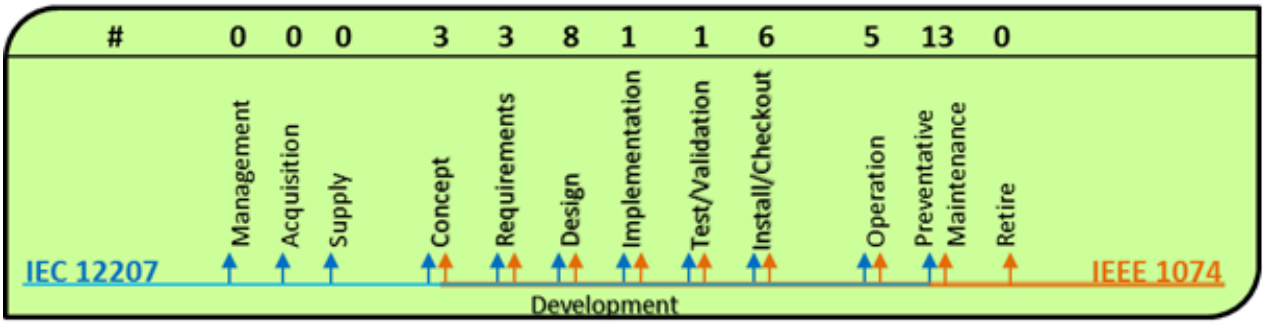
The short answer to this question of whether enough knowledge feedback from published events can improve safety of nuclear facilities is yes. Looking at the increased number of events published this past year the COMPSIS Steering Group sub-committee performed a study on forty of the ninety-nine

events using a natural root cause segmentation which employs a method that is aligned with the software lifecycle process.

Four main root causes were identified in this study and labelled as: hardware failures, human error, software failures and system issues. Each of these can be mapped back to the life cycle development model. Further a consequence analysis discovered three layer structures with events occurring in software application, the communication between system instrumentation and the equipment directly connected to the process. The study method analysis could very easily be realigned with several different classifications options such as: a component, system, or a plant level perspective. All of these potential study methods could increase our understanding while reflecting the published events on the life cycle development background.

Thus the event analysis are all based upon the events themselves, as a result, the segments are classified from predefined coding guidelines and demonstrates the errors that exist at all points in the life cycle (Figure 1.1). Approximately eighteen COMPSIS events were found related to hardware failures and human errors as they represent the operation and maintenance sections of the lifecycle, while the remaining COMPSIS events describe the software failures and systems issues and also exist as part of the life cycle process.

Figure 1.1: Events in a digital life cycle



From the study review of the forty events the following observations and lessons learned were made:

- Weaknesses in requirements are one of the most significant contributors to systems and software failing to meet the intended goals. A better analysis is needed to understand the software‘s interfaces with the rest of the system and discrepancies between the documented requirements for a correct functioning system.
- Performing software verification and validation, software safety analysis, and software configuration management can improve the software quality and enhance the software safety.
- Configuration data is a type of software. Configuration data shall be well managed during the whole software life cycle. If the software developers do not properly include configuration data, then software failures could be induced.
- False signal/Signal Interference issues are crucial events. The solutions to the issue are diverse, e.g. proper grounding, administrative control, shorting the unused I/O port or power line separation.

- Redundant architecture can cope with hardware single failure. Key improvements from lessons learned are: switch over time, completed channel redundant design, manual action in design, and preventative maintenance for hardware.
- Human/machine interactive errors are typical while modifying software and administrative control issues. It should be further observed with more events.

The study method in this report identifies a modest set of lessons learned. This study potential should not be considered the upper limit of the COMPSIS Project. It is the recommendation from this report that COMPSIS project continue adding more events and survey other study methods using the ninety plus events. The new COMPSIS website search option also provides ways to define alternative reviews of the data. These alternative views start with facility type, detection of an event, impact on people, environment and equipment, dependency, and cause classification, which a matured database could lead to new improvements in the prevention of future digital events.

ACRONYMS

ASIC	Application Specific Integrated Circuit
AVR	Automatic Voltage Regulator
CEAC	Control Element Assembly Calculator
CG	Coding Guidelines
CM	Configuration Management
COMPSIS	Computer-Based Systems Important To Safety
CPC	Core Protection Calculator
CPU	Central Processing Unit
CSNI	Committee on the Safety of Nuclear Installations
DIGREL	Digital Instrumentation and Control Reliability Task Group
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat
FPGA	New Digital Replacement Component
GRS	Gesellschaft für Anlagen- und Reaktorscherheit (German TSO)
HAEA	Hungarian Atomic Energy Authority
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I&C	Instrumentation And Control
I/O	Input/output
IFE	Institute for Energy Technology

ISTec	Institut für Sicherheitstechnologie (subsidiary of GRS)
MTO	(IFE) Sector Man-Technology-Organisation
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
O&M	Operation And Maintenance
OA	Operating Agent
OECD/NEA	Organisation For Economic Cooperation And Development/Nuclear Energy Agency
PRA	Probabilistic Risk Assessments
QA	Quality Assurance
SCM	Software Configuration Management
SG	Steering Committee
SQL	Structured Query Language
SSM	Strålsäkerhetsmyndigheten (Swedish Radiation Safety Authority)
STUK	Radiation and Nuclear Safety Authority of Finland
V&V	Verification And Validation

LIST OF FIGURES AND TABLES

1. INTRODUCTION/BACKGROUND

During the mid 1990s a Task Group was formed within the Organisation for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA), to exchange information on events involving computer-based systems important to safety in Nuclear Power Plants. The Task Group operated a trial database (MSAccess) to collect events involving computer-based systems important to safety in Nuclear Power Plants.

The lack of computer-based system failure data is still one of the major deficiencies in assessments of the risk of computer-based systems in nuclear facilities. To remedy this situation, it was highly important to establish the international Computer-Based Systems Important to Safety (COMPSIS) project. In 1999, the assigned task group issued a guideline document and a mission statement. By 2002 a COMPSIS task group was established to quality assure the new database. The OECD/NEA identified the requirements and the type of analysis will support risk analysis and the regulatory review of computer-based systems.

In 2005 the OECD/NEA Steering Committee agreed to establish the international COMPSIS project and encourage multilateral cooperation in collection and analysis of data relating to computer-based system events. The COMPSIS Project is designed to fill the shortage of computer-based system analysis data. This project will enable the identification of the root cause of a computer-based system failure and the effect of the failure and the determination of how the failure could have been prevented. The aim of the project is improving the safety of nuclear facilities by utilising operating experiences and providing common resources for analytical framework of qualitative and quantitative assessments. The type of analysis will support risk analysis and the regulatory review of computer-based systems.

The first period of the COMPSIS project has been concentrating on the development of clear definitions, coding guidelines, data base structure and user interface of the data base. In this period ten countries took part in the project. A progress report was issued at the end of this first period /2/.

The second period of the COMPSIS project has been concentrating on the collection of data provided by the project members. Unfortunately two countries left the project at the end of the first period. Nevertheless, substantial progress was achieved.

This report provides a brief overview of the current status of COMPSIS project. The results obtained are compared against the objectives of the project. Issues arising during the operation of the project are discussed and a perspective of the project is given.

2. SCOPE AND OBJECTIVES

The objectives of the COMPSIS project are given in the terms and conditions for the project /3/. In detail, the project's goals were:

a) to define a format and collect software and hardware fault experience in computer based safety critical NPP systems (hereafter called "COMPSIS events") in a structured, quality assured and consistent database;

b) to collect and analyse COMPSIS events over a long term so as to better understand such events, their causes, and their prevention;

c) to generate insights into the root causes and contributors of COMPSIS events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences;

d) to establish a mechanism for an efficient feedback of experience gained in connection with COMPSIS events including the development of defences against their occurrence, such as diagnostics, tests & inspections; and

e) to record event attributes and dominant contributors so that a basis for national risk analysis of computerized systems is established.

These objectives were not only defined for the first or second period of the project, but for long-term operation. Some of the goals in particular (e.g. b and e) need long-term operation of the database. The status of the project is described in the following chapters

During several Steering Group (SG) meetings the issue of the relatively small number of events compared to other data base projects have been discussed. To understand the situation of the COMPSIS project it is necessary to take specific conditions into account that result from computer technology like:

- Computerized systems important to safety are not yet implemented in all existing NPPs. Thus, lots of NPPs are still operated with several hard wired safety I&C systems.
- Computerized I&C systems are redundant systems. Single failures of e.g. one CPU in a redundant system are not always a failure of the system and may be not reported. For other equipment like pipes each leakage is a leakage also in redundant systems.
- Computerized I&C systems are complex systems. Root cause analyses may take much more time compared to less complex equipment.

In addition there exist specific conditions of the project like:

- Some countries operating large numbers of NPPs with digital I&C systems e.g. France, Japan, Canada are not participating in the project.
- In single member states of the COMPSIS project, National Coordinators have not enough resources to feed the database promptly.

Over and above these conditions, some stakeholders have excessive expectations regarding the usability of the short-term results of the COMPSIS project in probabilistic risk assessments.

3. STATUS AFTER THE FIRST PERIOD

3.1 Overview

The status after the first period is described in the report "Computer-Based Systems Important to Safety (COMPSIS) Project: 3 Years of Operation (2005-2007)" /2/.

During the first period, the participating members reported forty events that are collected in the data base. The reporting that was performed during the first period has to be seen as testing of the user interface and data base structure. The established guidelines and Web-based infrastructure is appropriate for input and archiving further data. A first attempt has been performed for qualitative analysis showing some results obtained from the collected events during the first period.

3.2 Results

At the end of the first period the following results have been obtained:

- Coding Guidelines V 3.2 have been established /4/, /5/.
- Data base has been established providing a Web-based user interface /6/.
- Web portal has been established (www.compsis.org).
- Operating procedures have been established /7/.
- QA procedures have been established /8/.
- Number of collected events: 40
  - Open events: 10
  - Pending events: 25
  - Event in approving stage : 11
  - Approved events: 4

A first evaluation of the events has been carried out. It shows that the majority of the events have been observed at non-safety systems/equipment or at systems/equipment of low safety importance.

4. PROJECT INFRASTRUCTURE

The Project Steering Committee (SG), composed of the national coordinators and additional experts of participating countries, manages the COMPSIS project. During the four years of the second period (01/2008–12/2011), the participants were AEC/INER/TPC (Chinese Taipei), STUK (Finland), GRS/ISTec (Germany), HAEA (Hungary), Consortium of KINS/KAERI/KHNP/KOPEC (Korea), SSM (Sweden), ENSI (Switzerland), and NRC (United States).

The SG holds all power to make project decisions. The OECD/NEA Nuclear Safety Division provides the secretariat services to the SG and handles financial matters and other types of administration for the project. Each country provides the funding that is generally used to finance the Operating Agent (OA, sometimes also referred to as clearinghouse) activities. The OA ensures the quality assurance and the operation of the database. It also prepares monthly progress reports to the SG. The Institute for Energy Technology (IFE) sector Man-Technology-Organisation (MTO) Safety, in Halden, Norway, acted as OA up to now. The SG has agreed to retain the services of IFE for the new three-year period (07/2011–06/2014).

In cooperation with the OA, the participants prepare project reports for general CSNI distribution. These reports are intended to contain conclusions on the analysis performed whenever major steps of the project have been completed. The COMPSIS SG approves all reports discussing the project data and/or findings. This document, the second COMPSIS project report, presents the achievements of the second period, 2008 until 2011.

The COMPSIS Terms and Conditions of the second period [2], also found in Appendix B, describes in detail the operation of the COMPSIS project. In particular, it addresses the responsibilities of the participants, the funding, and the distribution of the database.

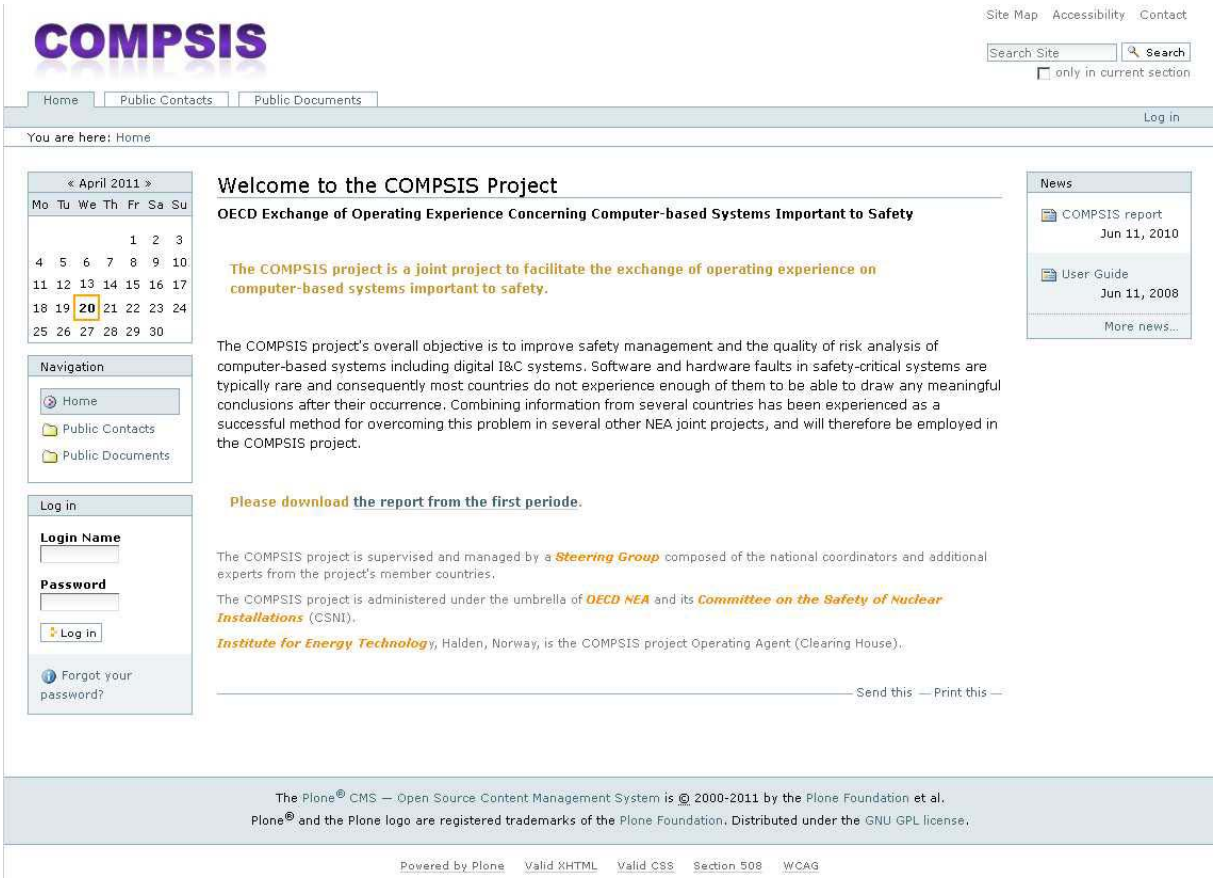
5. DATABASE CONTENT AND STRUCTURE

After the last upgrade of the server software, the SQL version of the COMPSIS database was updated. The list of words and expressions in the SQL syntax was expanded in the new version and a conflict between the naming of tables in the database and the syntax used in SQL was discovered. To resolve this conflict, the affected tables were renamed. In addition, the use of the wording and labels equal to that of the updated SQL syntax was changed in Zope/Plone. The contents of the renamed tables were however not changed.

6. THE COMPSIS WEB-PAGE

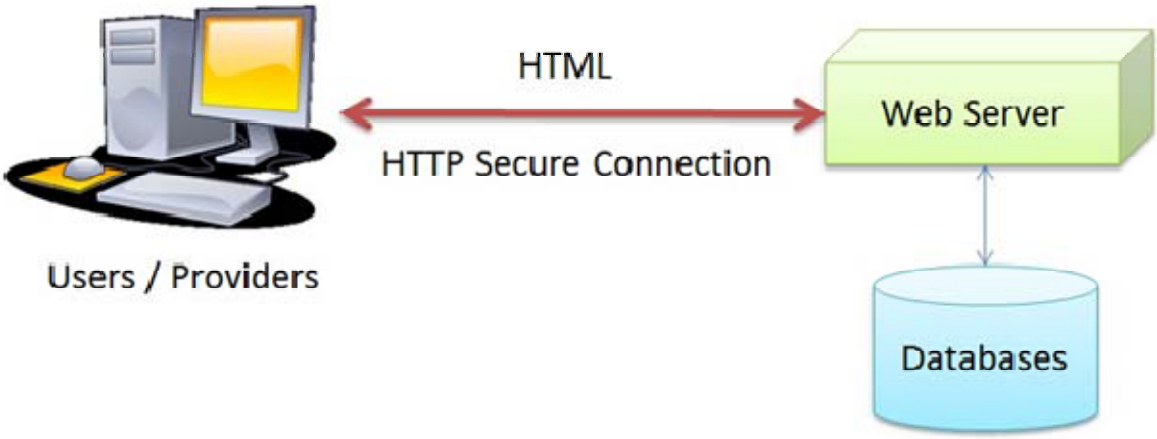
The activities of the COMPSIS project have been coordinated using electronic communication via e-mail and the COMPSIS Web-Page. It resided on its own domain "compsis.org". The welcome screen is shown in figure 6.1.

Figure 6.1: Welcome screen of the COMPSIS web-page



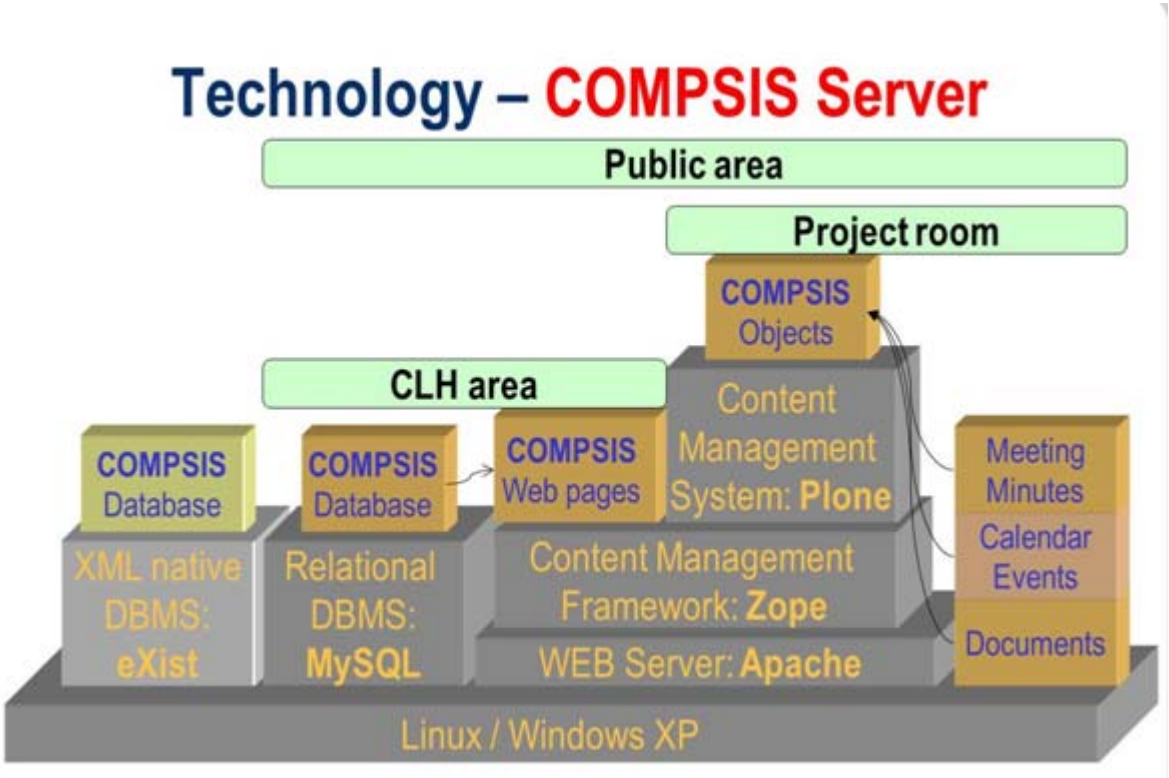
The Web page is divided in a public area, a confidential area (Projectroom) and an administration area (CLH area). Access to the web-page is secured by application of the HyperText Transfer Protocol Secure (HTTPS).

Figure 6.2: Web page - data base overview



The Web page is based on the use of open source software and runs on a Linux platform. The administrator can adjust the user rights in accordance to the users' roles in the COMPSIS project. The Web page allows files and documents to be stored and shared as required. In this way, the Web page is used as a project workplace in addition to giving members access to the database. In addition to controlling the members' user rights on the Web page, it is possible for the administrator to also control their access to the databases themselves, thus preventing users without the proper rights to access sensible data, and assuring that events can only be changed by the correct data providers.

Figure 6.3: Structure of the web-page



One of the main tasks of the web-page is to provide the user interface to the data base. The user interface enables data providers and the OA to control the complete life cycle of COMPSIS events.

The server is organised in two sections:

- One section is an x86 architecture server with Linux operating system running Apache as the foundation HTTP server. On top of Apache, there is a content management framework named Zope, which again is the foundation of a content management system called Plone. Apache, Zope and Plone are open source software, and provide flexibility, easy updates and high security.
- The second section of the server comprises the databases. On the Linux operation system, a MySQL server is installed. The MySQL software is also open source, and integrates well with the content management system.

The overview is given in figure 6.2.

7. DATA COLLECTION AND CURRENT STATUS

One challenge in setting up an international database is to ensure a consistent reporting level between countries in order to capture all events meeting the project criteria. Regulatory and utility reporting levels differ between member countries, and the reporting criteria may have changed with time. For events from the past, the database includes for reference the evolution of reporting levels over time. For future events, one objective of the first three-year phase is to define a project reporting level, which will account for the countries' policies while correctly addressing the technical objectives of the project.

With emphasis on data validity and data quality, the COMPSIS coding guidelines have been developed for collecting and classifying computer-based I&C system failure event data to ensure consistent interpretations and applications.

Each national coordinator is responsible for protecting and maintaining the proprietary rights of the information he or she provides to the project, including markings or other indications that such information is confidential. Every country arranges for the protection of proprietary rights. The Operating Agent is also bound to keep the proprietary information secure during the course of the project.

Compared to the objectives of the project the current status is as follows:

Table 7.1: Status of the COMPSIS project objectives

Objective	Current status
To define a format and collect "COMPSIS events" in a structured, quality assured and consistent database.	Completed, documents describing the procedures are available, database is working.
To collect and analyse COMPSIS events over a long term so as to better understand such events, their causes, and their prevention.	Ongoing process; current status see chapter 4.
To generate insights into the root causes and contributors of COMPSIS events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences.	The first analysis was performed at the end of the first project period /2/; an extended analysis is given in chapter 8.

Objective	Current status
To establish a mechanism for an efficient feedback of experience gained in connection with COMPSIS events including the development of defences against their occurrence, such as diagnostics, tests & inspections.	This process needs more experiences and may be an objective for a third period of the project.
To record event attributes and dominant contributors so that a basis for national risk analysis of computerized systems is established.	Ongoing process; connected to the analyses, data are available for national analyses.

The procedures to collect data are well established in the different member states. Additional procedures to remind data providers to publish events after approval have been established and are operated by the OA.

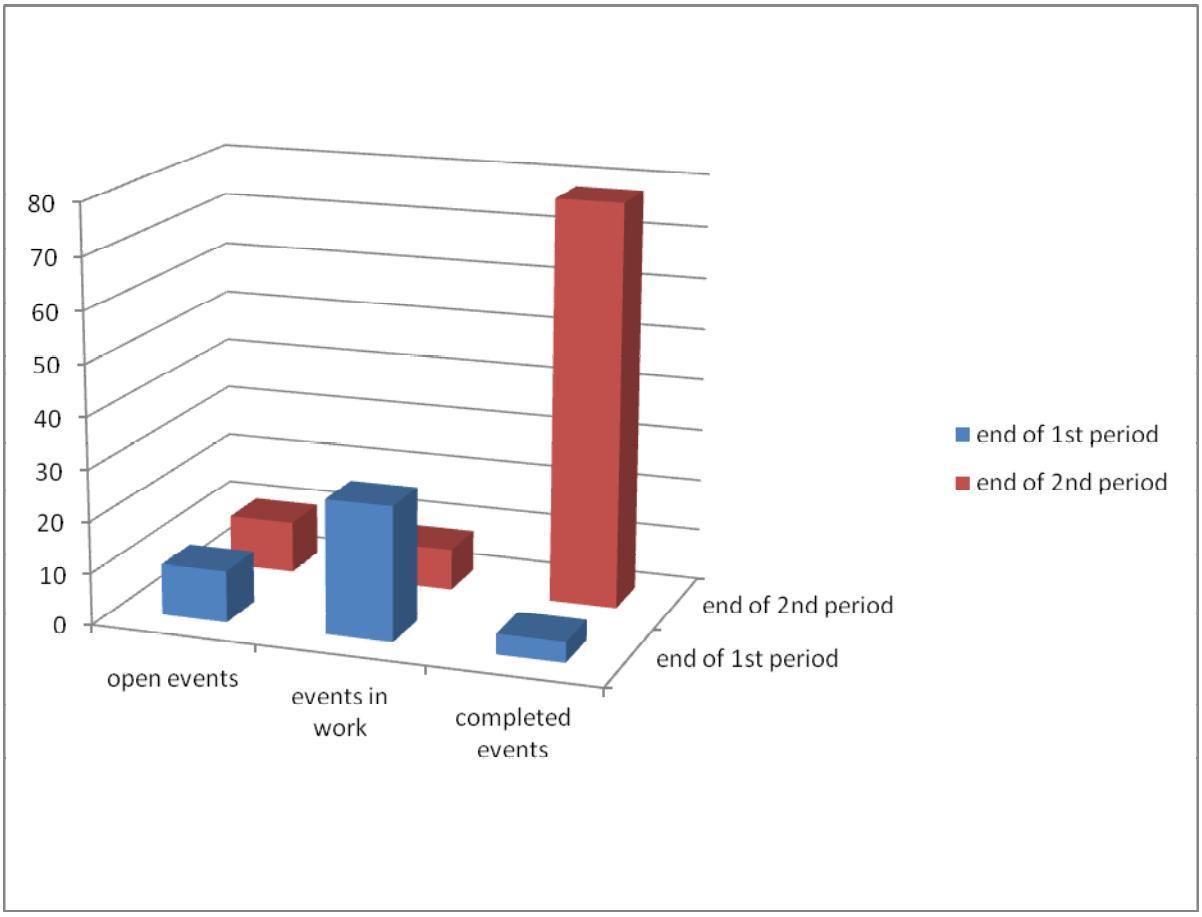
During the period 2008–2011, participating countries continued to deliver computer-based I&C system failure data to the COMPSIS project.

The number of events in the database has been increased. The statistics give the following figure:

- Number of collected events: 99
  - Open events: 4
  - Pending events: 3
  - Closed events: 0
  - Events in approving stage : 10
  - Published events: 82

Figure 7.1 shows the progress in data submission during the second period as compared to the first one. Significant progress in completing event analysis can be observed.

Figure 7.1: Progress in the collected events



8. QUALITATIVE ANALYSIS OF DATA AND OBSERVATIONS

8.1 Overview

Due to the progress of computer-based technology and the obsolescence and difficulty in maintaining analog control equipment, nuclear power plants (NPPs) are replacing their traditional electromagnetic and analog elements in their safety and control systems with programmable computer-based systems and equipment. The newer computer-based systems and equipment utilize technology with sensors, actuators, programmable hardware (e.g. field-programmable gate arrays) and software. These systems apply the advanced human-machine interface design, programmable hardware and software control technology to take the place of analog controls and instruments in conventional control rooms which require operators to survey many indicators, monitor the pump/valve status, and operate hard-wired actuator switches to keep the systems operated within a normal range or deal with abnormal conditions. Using the computerized instrumentation and control (I&C) systems and modernized main control room can often reduce the operator's burden and maintenance costs. Although computer-based design offers many advantages, some characteristics inherent in software and hardware integrated systems, human-machine interfaces, and project management may cause failure events during operations. Some of the computerized I&C system failure modes are different from those of conventional analog I&C system. These unanticipated failure modes could create very confusing situations that might place the plant, or lead operators to place the plant, in unexpected or unanalyzed configurations.

The objective qualitative analysis of Computer-Based Systems Important to Safety (COMPSIS) event data is to comprehend the root causes and consequences of computerized I&C system events, which are collected from the member countries of COMPSIS project on related events that may affect the safety of NPPs.

8.2 Analysis for selected characteristics

For software based systems specific characteristics of events are of general interest. The following table gives a short overview about selected characteristics.

Table 8.1: Selected characteristics

Characteristic	Area/Type	Number of events
Root cause belongs to	Hardware	31
	Software	12
	Commands	5
Temporal behaviour	Transient	34

Characteristic	Area/Type	Number of events
	Permanent	33
	Intermittend	15
Dependency	Single failure	47
	Multiple failure	7
	Systematic failure	2
	Common cause failure	16
	Independent failure	1
	Dependent failure	8

The analysis is based on the published 82 events.

8.3 Study on root causes and consequences analysis

This study was performed in May 2011. A total of forty events were investigated to identify the root causes and perform consequences analysis. After analyzing the forty events, it was concluded that there were four root causes and thirty five causes. The analysis used the low-level deficiency code of the event Coding Guidelines (CG) to categorize those causes. More detailed descriptions of the root causes and consequences analysis appear in the following subsections.

8.3.1 Root causes

8.3.1.1 Hardware failure

Hardware failure is one of the most common causes. It can be a loss of control function for the computerized I&C system itself, loss of software in the storage device (memory or hard disk), or a false signal/signal Interference to other I&C systems. In this analysis, two COMPSIS events are involved in loss of control function for the computerized I&C system itself, a COMPSIS event is involved in loss of software in the storage device, and four COMPSIS events are involved in false signal/signal Interference to other I&C systems.

(1) Loss of control function due to hardware failure:

(i) A hardware failure of converter in automatic voltage regulator (AVR) induced loss of voltage control, and eventually a reactor scam. The converter is a common component for both of the redundant channels. Therefore, a completed channel redundant design is recommended to resolve the hardware failure of converter. It means a dedicated converter for each redundant channel.

(ii) A control card hardware failure of the steam generator level control system induced fully open of feedwater control valve. Eventually, the reactor scrammed due to low steam generator water level. The control circuit card can use the redundant architecture to avoid signal failure.

(2) Loss of software in the hardware storage device: A COMPSIS event shows the operative software was lost in the programmable logic controller when the controlled machine was going to be taken into operation. As a result, the machine did not start.

(3) False signal/signal Interference to other I&C systems: The related events are analyzed in the "False signal/Signal Interference" section.

8.3.1.2 Human error

In this human factor cause, the study found that some events stem not only from human factors but also from other causes. However, personnel can avoid this type of event by taking more care.

(1) Operation error: In spite of there being defects in system design, personnel can avoid operation error by being more attentive. Three COMPSIS events are involved in Operation error:

(i) A wrong numeric value had inadvertently appeared in connection with user software modifications, probably as a result of a typing error.

(ii) During the replacement of a failed AVR controller for generator exciter, a maintenance technician unintentionally injected the flash light beam into the end of fiber optic cable for the AVR main controller which resulted in the failure of exciter and main generator.

(iii) The test switches on a rod position indicator were left in test position after the completion of the maintenance procedure during an outage. The unit was tripped because the digital rod position indicator was inoperative.

(2) Unauthorized Operation: The operation should follow the procedure to manipulate the control system. Unauthorized operation, which is not verified or approved, can induce an event. A COMPSIS event is identified as unauthorized operation, an operator used an un-approved control function. As a result, a fuel bundle was inclined due to loss of control.

(3) Operator command error: The shift manager made a command decision to trip the plant based upon the miss interpretation of an operator's explanation to a question. The concern was over an incomplete software verification for the control element assembly calculator (CEAC) functions, which feeds into the core protection calculator. The CEAC was not required at this mode of plant operation. This information was not considered and led to the incorrect conclusion and site shutdown.

Another COMPSIS event describes the lack of understanding of technical specifications for testing the digital CEAC. This event was recorded as a human error and demonstrates complexity involved with digital equipment.

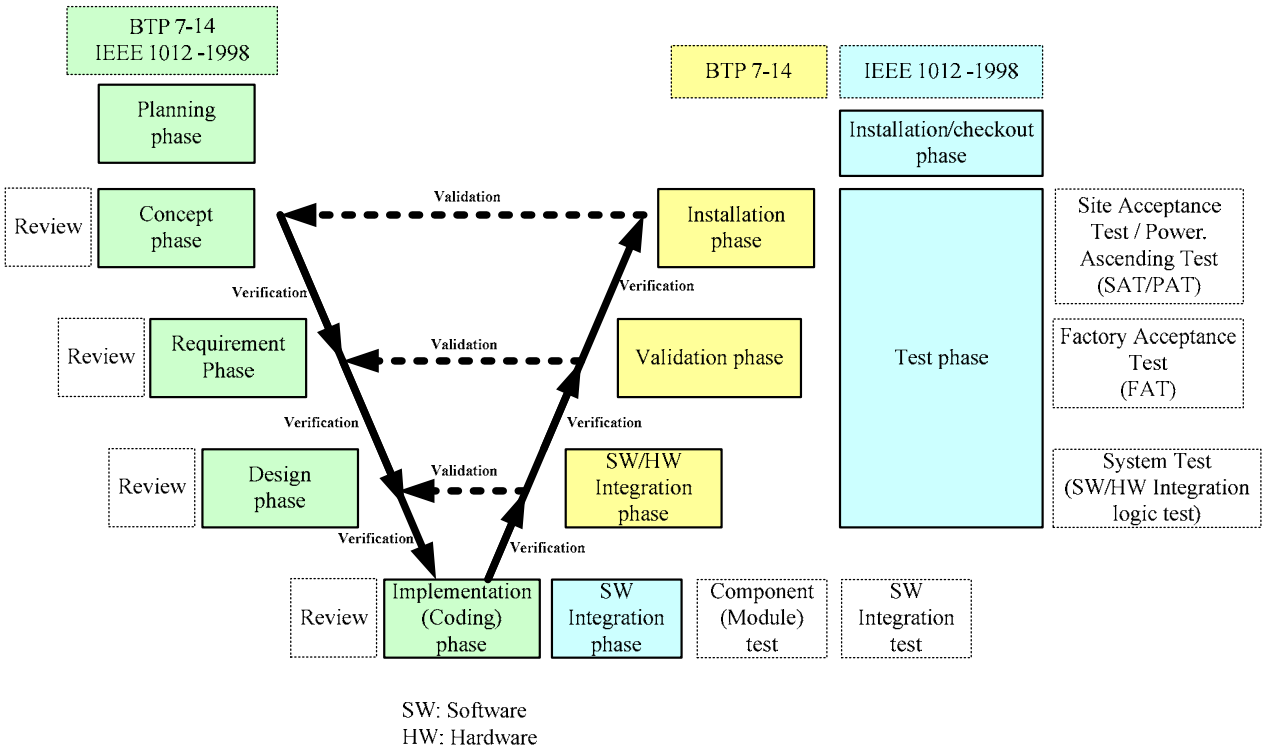
8.3.1.3 Software failures

Software Development life cycle

The industry standards1 identify the development of life cycle phases, such as, planning phase, requirement phase, design phase, implementation phase, integration phase, validation phase, installation phase, and operation/maintenance phase. There are specific activities for each phase. The developer of digital I&C system should evaluate the impact, if a modification is needed. For example, in installation phase, the functional requirement should not be changed without completely evaluation.

The developer of digital I&C system should follow the planned activity of each phase in the life cycle. The software verification and validation (V&V) team should perform the V&V work to ensure sufficient reliability of the digital I&C system software. Figure 8.1 shows an example of phases of software development lifecycle.

Figure 8.1: Example of phases of software development lifecycle



There are several COMPSIS events related to the software development lifecycle. Each area discussed below demonstrates the connection between events and the software and system life cycle.

[1] See IEEE Std. 1012-1998, IEC 60880, and IEC 61513.

The segmentation of these COMPSIS events in the future will demonstrate new ways to prevent the types of failure outline below:

(1) Planning and Concept mistakes: Planning a digital system from the very start requires an understanding of what digital controls can and cannot do. One COMPSIS event demonstrates this error by the use of a digital system design to overcome other system intermittent power interruptions. The use of digital does not resolve the original system issue.

Two other COMPSIS events demonstrated concept phase mistakes by the application of incomplete and incorrect digital technology. The lack of a de-bouncing algorithm pushbutton sent an operator's reactor level command way beyond the intended set point, while the incorrect logic string application of a turbine runback resulted in losing control of the turbine. In both situations the NPPs tripped with significant stress on the operating staff.

(2) Software defect in requirement and design phase: Please refer to "8.3.1.3.2 Software defect in requirement and design phase"

(3) Software fault in implementation phase: A faulty implementation of the algorithm resulted in a sudden abrupt rise of the output signal. The algorithm had not been implemented in line with the design specifications. The V&V team did not identify this software fault.

To prevent this kind of software fault, a solid software verification and validation should be performed. The traceability analysis in implementation phase can identify the inconsistence between software implementation (source code) and software design. The hardware/software integration test should identify whether such software defects are in the code.

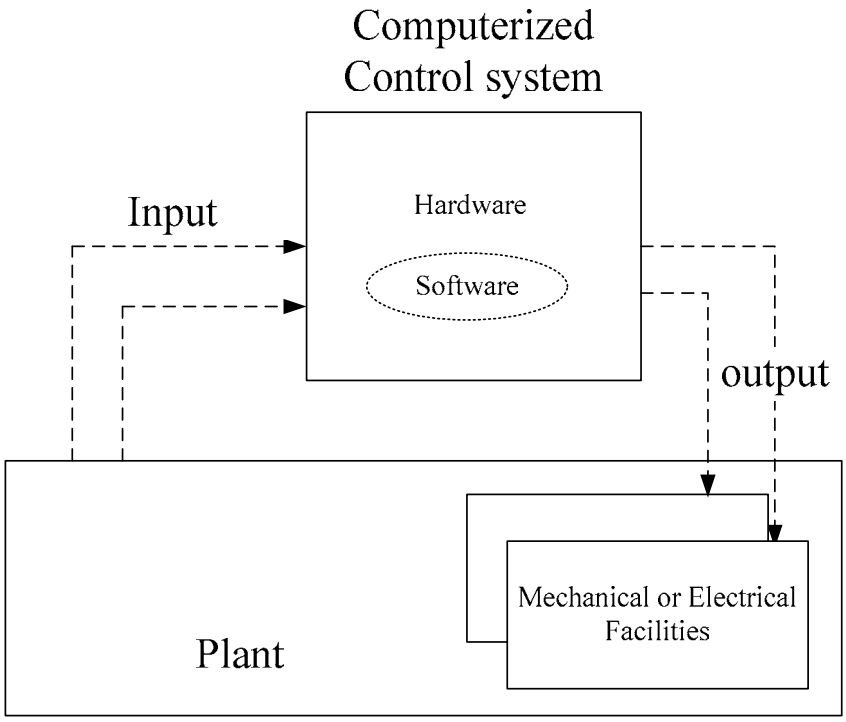
(4) Fail to identify software fault in validation phase: A factory acceptance testing in validation phase with good completeness can identify software defects which are introduced in the design phase. These defects might induce system failure in the operation and maintenance (O&M) phase.

(5) Software Configuration management (SCM): SCM should be performed in the Software development of life cycle. Please refer to "8.3.1.3.3 Software Configuration management".

Software defect in requirement and design phases

Software defect in requirement and design phases are the major impact factors for computer-based safety system. The main reason leading to this cause is negligence concerning system requirements. The undesired result is that many more efforts are needed to make up for the previous mistakes in the requirement analysis phase. Figure 8.2 shows a simplified relationship between the computerized control system and the controlled facilities of plant. In the computerized control system, software is implemented in the hardware, which controls the mechanical or electrical facilities, such as, pumps, valves, positioner, or generator. As a result, incomplete consideration on the mechanism of controlled facilities would induce system failure. Thus, when planning to add a new function or remove an existing function, the functional requirement should be carefully analyzed.

Figure 8.2: Simplified relationship between the computerized control system and the controlled facilities of plant



There are six COMPSIS events involved in software defect in requirement and design phases:

(1) A software requirement was changed without considering control valve positioner mechanical failure while performing feedwater controller digital replacement. As a result, a reactor scram was induced by loss of the reactor water level control.

(2) The mechanical path and the physical dimension of a refueling machine were not completely analyzed in the software requirement phase. This requirement defect was not identified in the validation test phase. As a result, a mechanical damage was induced by this design defect in O&M phase.

(3) The power plant personnel requested the software developer to improperly change the software requirement of a refueling machine. Consequently, a system operation failure was induced by this change.

(4) A software erroneously attempted to transfer the result of a division (which was 0.5) to an integer. This induced an unexpected mechanical motion.

(5) Erroneous memory addressing is not precluded, because the programmer has access to the whole memory space including the system area. High quality of Software design is important to the operational Software too.

(6) An installed core protection calculator (CPC) software was not consistent with the system software requirements document. Consequently, all four channels of the CPC were declared as inoperable. To prevent this kind of software fault, a solid software verification and validation should be performed. The traceability analysis in design phase can identify the inconsistence between software design and software requirement. The validation test can identify whether the software requirement is completely fulfilled or not.

Software Configuration management

Traditionally, the goal of configuration management (CM) programs is to ensure system consistency throughout the operational life cycle phase, particularly as changes are being made. Software configuration management (SCM) can be regarded as a subset of general CM in computer-based systems. Similarly, SCM is a process that is involved with identifying configuration items, changes control (including impact analysis), status accounting, and auditing. Its aims are to maintain integrity and traceability of the configuration items throughout the software Development of life cycle. However, impact analysis and safety evaluation were often ignored in the real world. Some failures are induced by neglecting the comparability with other functions when adding a new function. In addition, the records of change and test reports were missed in the software maintenance environment. More specific descriptions are listed below:

(1) Impact analysis: For a complex system, impact analysis should identify all configuration items which will be impacted before any configuration item is changed.

(2) Status accounting/auditing: The authors recommend that an SCM team be responsible for managing and controlling the status of a change request in a nuclear power plant. Any updates to change requests and software baselines should be performed under authority of the SCM team. The assessment result, such as reject, accept, or pending, will be recorded as the change request status and returned to the owner of the change request by the SCM team.

A COMPSIS event shows deficient software version management. The reloaded software version was not the correct one. It induced an erroneous initiation of protection limit action. While two other COMPSIS events demonstrated that the proper core protection calculator values for the latest fuel cycle can also be loaded incorrectly. A proper configuration and version management is an essential basis for the maintenance of the computer based systems.

Configuration data

The configuration data are identified as a kind of software, such as, setpoint values, ratio and timing constants, input/output (I/O) card address ports, priority and alarm settings, or any control parameters and tunning constants, they should be properly defined in system/hardware/software requirement phase, and evaluated/tested in installation phase.

(1) Address of I/O port: An incorrect I/O port address was composed in the application software. As a result, a component was locked incorrectly due to the wrong I/O port address.

(2) Priority setting: A COMPSIS event which involve a false network failure alarm message, was identified as improper software priority setting.

(3) Wrong parameter setting value: A wrong numeric value was input by the software user. The limit switch of a digital control system was not effective in the correct direction.

8.3.1.4 System issue

False signal/Signal Interference

In this COMPSIS event analysis, false signal/signal interference can lead to loss of control or spurious trip/actuation. The cause of false signal/signal interference can be hardware failure, improper signal separation, light interruption in fiber optical cable, interface compatibility problem, or software failure.

(1) Light interruption: A maintenance technician unintentionally injected the flash light beam into the end of fiber optic cable for a controller which resulted in controller failure. Administrative control and maintenance training should include this unintentional signal injection.

(2) False actuation signal: A memory read/write errors in the communication cards sent the false actuation signal to the controller card, which induced failure of reactor coolant pumps and reactor scram.

(3) Signal interference: Three COMPSIS events are identified as signal interference.

(i) A hardware failure of excitation module induced a noise signal, which was propagated through power line to other excitation modules. A spurious reactor scam was induced eventually. The separation (e.g. system power lines separation) for preventing signal interference should be included in the system/hardware design for each module was separated independently.

(ii) An unused, open, I/O port sent a high noise current signal, which induced a false protection action, and eventually induced a reactor scam. Signal interference might exist in some open/unused I/O port. In order to prevent false signals, the I/O ports, which are not used, should be shorted.

(iii) An improper grounded inverter induced interfering signals which blocked the input channel of feedwater pump controller. The feedwater pump then changed to manual mode from automatic control mode. Eventually; the reactor scrammed due to low reactor water level. The grounded test should be performed before the installation or replacement of new devices or equipment. The digital control cabinet should be well shielded to prevent spurious interfering signals. The specification of grounding and shielding should be preliminarily proposed in requirement phase.

(4) Interface incompatibility: Two COMPSIS events are identified as interface incompatibility. To prevent the incompatibility issue, interface analysis should be performed for the newly replaced component/system in the requirement phase and design phase.

(i) A new digital replacement component (FPGA) has interface compatibility problem with the other existing components (ASIC). Interface analysis and test are necessary for avoiding signal interference, signal interruption between components.

(ii) A communication circuit board was replaced in the automatic voltage regulator (AVR) system. The new communication circuit boards were incompatible with the original system design. This incompatibility resulted in the blocking and isolation of one of the three thyristor converter units. Consequently, a main generator trip with subsequent main turbine trip and reactor scram. To resolve this incompatibility issue, the new communication circuit boards were replaced with the original circuit boards. A filter (Ferrite bead) was added on the signal cable to filter out high frequency noise and reduce susceptibility to internally and externally generated electronic noise.

(5) Electromagnetic interference: No electromagnetic interference is identified in this analysis.

(6) False data link: The appearance of a fully operating core protection calculator however the date link to the core monitoring computer failed and thus the channel surveillance requirements were not performed. The issue was a component failure and a contributing factor is how the software program methodology for calculating deviations between channels is performed.

Communication failure

In this COMPSIS event analysis, communication failures resulted in loss of control for the control system and sending false actuation signal. The root causes are (1) excessive traffic on the network; (2) unintentionally injected the flash light beam into the end of fiber optic cable; (3) memory read/write hardware errors in the communication cards; and (4) communication circuit board interface incomparability. The last three events are included in "False signal/Signal Interference" section.

(1) Excessive traffic on the network: An excessive traffic on the connected plant Integrated control system network resulted in loss of power providing to the reactor recirculation pump motors. Consequently, the operator scram the reactor manually. The network traffic analysis should be performed to prevent this communication failure.

Redundant architecture

The redundant design is to cope with software/hardware single failure. The redundant architecture can be defeated due to improper design or setting.

(1) Hardware single failure: Redundant architecture can resolve hardware single failure issue. A COMPSIS event shows that a steam generator level control system made the false signal for the feedwater control valve. The root cause was the hardware failure of control card. In this case, a triple redundant design can resolve the hardware single failure by comparing the output signals.

(2) Switch over time: Improper switch over time (too short or too long) would induce failure of switch over from primary channel to backup channel. There are two sets of COMPSIS events (five total events) at a particular site with a hardware fault mechanism listed as the cause for the very first event, however with further analysis it becomes evident that there is a sequence of failures which leads to a vender equipment solution with the internal digital design. These types of events appear as power supply transitions to a backup or a control card replacement while depending on the back up computer for a bump-less transfer. The design fault can be a software configuration management or vulnerabilities with the processors.

(3) Completed channel redundant design: A completed channel redundant design is recommended. If there exists a common component for both channels, the failure of common component will defeat the redundant architecture. A COMPSIS event shows that a failure of common component of the AVR redundant architecture, which induced the failure of both primary and backup channel.

(4) Analog component: Analog component is recommended for watchdog timer and switch (used for switching from primary channel to backup channel) in the redundant design. Software failure of digital watchdog timer and switch can induce a software common failure in the architecture.

(5) Manual action: Manual action can be considered in a redundant design. For example, if the primary fails, the backup would take over. When the system is back to normal, the operator should switch to the primary manually. A COMPSIS event shows that the automatic switching back to primary channel function could not resolve the mechanical failure of positioner.

(6) Preventive Maintenance: Preventive maintenance is recommended to keep the backup channel be available. Some unstable symptoms can be observed before a hardware failure, in this case, conservative decision making is recommended to replace the hardware. Several turbine system COMPSIS events show the failure shows the backup channel of turbine control digital electro-hydraulic system had malfunctioned while switching from primary channel to backup channel. The unstable symptoms of the backup channel had been observed before the event.

8.3.2 Consequences analysis

In this consequences analysis, the authors referenced the system description section of the CG /4/ and adopted three layers of system structure—application, communication, and process and the system element to represent observed and possible consequences. The results appear in Table 8.2. In addition, the analysis results of corrective actions are also shown as Table 8.3

Table 8.2: Observed and possible consequence

Root cause (area)	Structure layer	System element
Development of life cycle	Application, Process	Controller, Actuator, Sensors/Transmitter Application software, System software
Design defect	Application	Controller, Application software, System software
Configuration management	Application	Application software
False signal/Signal Interference	Communication, Process	Controller, Actuator, I/O, Application software
Communication	Communication,	Interface card

Root cause (area)	Structure layer	System element
	Process	
Hardware failure	Process	Controller, Actuator, Sensors/Transmitter
Human factor	Application	Human-machine interface
Configuration data	Application	Application software
Redundant architecture	Application, Process	Controller

Table 8.3: Corrective actions

Root cause	Corrective actions
Development of life cycle	Follow the activities in each phase of life cycle. Perform Verification and Validation (V&V) in each phase of the software development of life cycle.
Design defect	Analyze the function of design.
Configuration management	Fulfill software engineering concepts and practice.
False signal/Signal Interference	Signal shielding to prevent spurious interfering signals. Signal interference should be included in the system/hardware design.
Communication	Perform environmental test in advance.
Hardware failure	Redundancy design and implementation.
Human factor	Enhance training and knowledge management.
Configuration data	Properly defined the configuration data in requirement phase, and evaluated/tested in installation phase.
Redundant architecture	Enhance and confirm the redundant design.

8.4 General Recommendations

By means of the qualitative analysis, the general recommendations are proposed as below:

(1) Analysis of the COMPSIS events (see section *8.2.1.3.2)* have shown that weaknesses in requirements as one of the most significant contributors to systems and software failing to meet the intended goals. There is a need for analyst to better understanding of the software's interfaces with the rest of the system and discrepancies between the documented requirements needed for correct functioning of the system.

(2) Performing software verification and validation, software safety analysis, and software configuration management can improve the software quality and enhance the software safety.

(3) Configuration data are a kind of software. If the software developer does not properly deal with configuration data, a software failure could then be induced.

(4) False signal/Signal Interference issue is crucial in the COMPSIS event data. The solutions of the issue are diverse, e.g. proper grounding, administrative control, shorting the unused I/O port or power line separation. However, they are mostly hardware failures. The solutions are similar to that of analog system.

(5) Redundant architecture can cope with hardware single failure. However, in order to keep the redundant architecture available, some key points should be noticed, such as switch over time, completed channel redundant design, manual action in design, and preventive maintenance for hardware.

(6) No direct human/machine interactive error in main control room is reported in this phase, the human error in the COMPSIS events are typing error while modifying software and administrative control issue. It should be further observed with more events.

9. RECOMMENDATIONS FOR THE FUTURE

9.1 COMPSIS Project

The SG is convinced that it is worthwhile to continue the COMPSIS project for a 3rd period. Increasing numbers of events are expected mainly due to:

- increasing implementation of computerized safety I&C in NPPs;
- increasing implementation of safety related computerized I&C with reduced level of qualification.

Nevertheless, it is expected that the number of events in the database grow moderate and thus, building a database useful for quantitative data analysis may take a decade. However, the COMPSIS project members believe that the project can have an significant influence for the future.

9.2 Collaboration with DIGREL

After the 9th Steering Group meeting of the COMPSIS project the chairman contacted the task leader of the DIGREL task group. This task group aims at bringing forward the development of methods for the modelling of software based digital I&C in probabilistic risk assessments (PRA) by developing a common taxonomy of failure modes. Both sides are convinced that the COMPSIS project and the DIGREL task group complement one another and can benefit from each other, e.g. COMPSIS events could be used to assess the completeness and adequacy of failure mode taxonomies developed in the DIGREL task and the taxonomy of failure modes developed in DIGREL may be integrated in the COMPSIS data bank when the COMPSIS coding guideline is developed further. The mutual information of both projects on the other projects' development is ensured by one national coordinator being also participating in the DIGREL task group.

10. CONCLUSIONS

The given report describes the status of the COMPSIS project and the progress obtained during the first two periods of operation (2005-2011).

The procedures to collect data are well established in the different member states. Procedures to avoid unnecessary delay in event processing have been established and are operated by the OA.

Working through second COMPSIS project period (2008–2011), organisations from Finland, Germany, Hungary, the Republic of Korea, Sweden, Switzerland, the United States and Chinese Taipei took part. The participating countries continued to deliver computer-based I&C system failure data to the COMPSIS project.

During the first project period the framework of the project (Coding Guideline, Databank, Web-Interface) was established and data collection was started. The second project period's main focus was on collecting data. Thus, the amount of events in the databank increased substantially from twenty two events after the first project period to ninety-nine. It is expected, that the number of events in the database will increase moderately in the future due to increasing implementation of computerized safety and safety related I&C in NPPs.

During the second project period communication with the DIGREL task group was established. This task group aims at bringing forward the development of methods for the modelling of software based digital I&C in probabilistic risk assessments (PRA) by developing a common taxonomy of failure modes. Collaboration of the COMPSIS project with the DIGREL can improve the results of both groups in the future.

The study method in this report identifies a modest set of lessons learned. This study potential should not be considered the upper limit of the COMPSIS Project. The COMPSIS project has the potential of adding more events and surveying other study methods that will provide other insights. Using the new COMPSIS website search option also provides another way the COMPSIS Project can investigate the event relationships. These are events that can cluster and/or sequence for one particular power plant or systems. The alternative views with the search option start with facility type, detection of an event, impact on people, environment and equipment, dependency, and cause classification, and these options in the matured database could lead to new improvements in the prevention of future digital events.

The members of the COMPSIS project would like to express their opinion that it is worth to continue the project with a 3rd period of operation.

11. REFERENCES

[1] Measurement Uncertainty - Methods and Applications, Third Edition, R. H. Dieck. The Instrumentation, Systems, and Automation Society, Research Triangle Park, North Carolina, 2002.

[2] Computer-Based Systems Important to Safety (COMPSIS) Project - 3 Years of Operation (2005-2007) NEA/CSNI/R(2008)13.

[3] OECD Exchange of operating experience concerning computer-based systems important to safety (COMPSIS) project - Terms and conditions for project operation 2008-2010, 2007 (NEA/SEN/SIN/COMPSIS(2007)1).

[4] COMPSIS - OECD Exchange of Operating Experience concerning Computer-based Systems Important to Safety at NPPs, Event Coding Guidelines, Version 3.2 / OECD, 2008.

[5] Computer-based Systems Important to Safety (COMPSIS) / OECD/NEA. Paris, 2000 - Reporting Guidelines.

[6] COMPSIS DataBank (3.2), User Guide (1.0) / COMPSIS Clearing House, 2007.

[7] OECD-COMPSIS Operating Procedures / OECD, 2009.

[8] OECD-COMPSIS Quality Assurance Program / OECD, 2009.