Unclassified **NEA/CSNI/R(97)23**

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

OLIS : 08-Sep-1998
Dist. : 10-Sep-1998

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(97)23
Unclassified

OPERATING AND MAINTENANCE EXPERIENCE WITH COMPUTER-BASED SYSTEMS IN NUCLEAR POWER PLANTS

A report by the PWG-1 Task Group on Computer-based Systems Important to Safety

English text only

68831

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

ABSTRACT

This report was prepared by the Task Group on Computer-based Systems Important to Safety of the Principal Working Group No. 1. Canada had a leading role in this study.

Operating and Maintenance Experience with Computer-based Systems in nuclear power plants is essential for improving and upgrading against potential failures.

The present report summarises the observations and findings related to the use of digital technology in nuclear power plants. It also makes recommendations for future activities in Member Countries.

Table of Contents

1. INTRODUCTION

Continued expansion of digital technology in nuclear power reactor has resulted in new safety and licensing issues, since the existing licensing review criteria were mainly based on the analogue devices used when the plants were designed. On the industry side, a consensus approach is needed to help stabilise and standardise the treatment of digital installations and upgrades while ensuring safety and reliability. On the regulatory side, new guidelines and regulatory requirements are needed to assess digital upgrades.

Upgrades or new installation issues always involve potential for system failures. They are addressed specifically in the "hazard" or "failure" analysis, and it is in this context that they ultimately are resolved in the design and addressed in licensing. Failure Analysis is normally performed in parallel with the design, verification and validation (V&V), and implementation activities of the upgrades. Current standards and guidelines in France [1], U.S. [2] and Canada [3] recognise the importance of failure analysis in computer-based system design. Thus failure analysis is an integral part of the design and implementation process and is aimed at evaluating potential failure modes and cause of system failures. In this context, it is essential to define "System" as the plant system affected by the upgrade, not the "Computer" system. The identified failures would provide input to the design process in the form of design requirements or design changes for the new installation or the upgrade. Procedures, training, and other practices, as well, may be affected by the failure analysis because administration controls, periodic calibration and surveillance procedures may all be used to provide defence against potential failures.

An important input to the failure analysis activities comes from the feedback of operating and maintenance experience. Feedback of operating experience in nuclear power plants has long been recognised as a valuable source for improving system design, procedures or human performance to achieve safety and to prevent recurrence of failures. This is particularly true in the case of complex systems such as computer-based systems. The process of feedback would provide designers with information on systems failures, unforeseen scenarios, or unanalysed configurations.

The review of operating experience and the identification of causes of failures is also essential for the regulators in performing their safety assessments. Currently, the NRC reviews the electromagnetic compatibility (EMC), software reliability, and the human-machine interface when it performs a safety evaluation of digital upgrades to ensure that the digital system failures resulting from the identified causes are within the acceptable level of a system’s reliability.

Operating experience with computer-based system is one of the topics raised in the SESAR report. The CSNI Bureau of the OECD has requested NEA Principal Working Group No. 1 (PWG1) to review this topic. A task group led by Canada was therefore formed within PWG1, including France, Japan, U.K., and U.S.A. to address the related issues.

The purpose of this report is to summarise the observations and some findings related to the operating and maintenance experience, based on contributions from France, U.S.A., U.K., Japan, and Canada. Additional information from the review of the open literature is also included. A number of the operational incidents, selected as case studies, are presented as examples in Appendix 1. In addition, this report presents an example of an evaluation by the US NRC of the digital upgrades introduced at an operating nuclear power plant.

2. CONTRIBUTIONS FROM OECD COUNTRIES PARTICIPATING IN THE STUDY

United States of America

In the U.S.A., the nuclear industry and the NRC have performed numerous studies of digital systems to identify safety concerns and to minimise failures of Computer-based systems. These studies were in response to the replacement of analogue instrumentation and control (I&C) systems with computer-based digital I&C systems by the utilities. Recent efforts in the US nuclear industry related to computer-based systems included the following:

- The National Academy of Science has completed a review of digital systems in the US nuclear industry.

- The Standard Review Plan, NUREG-800, Chapter 7, Instrumentation and Control, is currently being updated to include digital systems.

- The US NRC has begun compiling quarterly reports on the digital problems in the nuclear power plants.

Reference [4] , which was submitted as a contribution to this study, describes the results of one of the US studies on computer-based digital system failures and evaluates the NRC's review of analogue-to-digital conversions. The U.S. study focused on the current operating experience of computer-based systems in the U.S. nuclear industry as reported to the NRC. The purposes of the study were (1) to identify the types of digital system failures and (2) to ascertain how the NRC reviews digital updates. The first purpose involves reviewing Licensee Event Reports (LERs) involving digital failure events experienced in 1990-1993, and categorising digital system failures. The second purpose involves reviewing Safety Evaluation Reports (SERs) for analogue-to-digital upgrades, one for a General Electric plant and another for a Westinghouse plant. The review of 79 applicable LERs resulted in four categories of failures: software error, human-machine interface, Electromagnetic Interference (EMI), and random component failure. Software errors were further divided into software V&V (verification and validation) failures and configuration control failures. A description of each category follows in section 3.

Canada

In Canada, an in-depth review of the Canadian operating experience with CANDU computer-based systems was initiated to address the safety issues arising from the use of these systems [5]. This review was based on the experience collected from the Atomic Energy Control Board's (AECB's) analyses and reviews of CANDU significant events over the past 13 years. The review of 459 significant event reports from 22 reactor units, related to computer-based control, monitoring and safety-systems, was undertaken to identify types of failures encountered to date, lessons learned through operating experience, measures taken to address known software/hardware weaknesses, the impact of human interaction on software/hardware performance and the effectiveness of past computer expansion, upgrade and replacement programmes.

While the review covered a relatively large number of computer related events, it should be recognised that they do not necessarily include all computer failures. They include only those events which resulted in consequences that meet reporting criteria of either the AECB or the utility. Most hardware, for example,

is duplicated, and a single failure of a redundant component generally would not be reported formally to the AECB but would be reported internally in the utility.

France

In France, the experience of IPSN in evaluating the safety submissions from EDF related to the assessment of I&C systems were reviewed [1]. The review presented the methodologies used, including approaches for the identification of failures and management of modifications.

An additional contribution to this study consisted mainly of an IPSN evaluation report on the recent installation of a "computer-based monitoring and control" (KIC) system for use in the main control room of two units (B1 and B2) of the Chooz nuclear station. The human aspects associated with this new KIC system were included. IPSN also presented a functional study based on significant incidents which occurred between 1985 and 1993 and involved the Controbloc system (PLC - Programmable Logic Controller - in use for 1300 MWe nuclear power plant operation) to assess the consequences of significant incidents on safety.

The report provides a description of the new KIC system, a description of one of the final phases of the testing performed before the KIC system was installed in the Chooz B1 unit, and a summary of the experience gained following the installation of the KIC system. For the purpose of this study, the generic lessons learned from the testing phase and following the installation of the KIC system were collected and documented.

The final phase of the pre-installation testing was performed using a full scope training simulator. Although the simulator was not an exact replica of the control room where the KIC system was to be installed, the differences were identified and considered for the evaluation. A total of 12 scenarios comprising both transient and accident conditions were used for the test. Each scenario was run with 4 different crews for a total of 48 test runs.

The post-installation testing campaign looked at the performance of the KIC system following its installation in the Chooz B1 and B2 units. Different versions of the KIC system were installed with the most recent version installed in the B2 unit. Many improvements and modifications were made as a result of the testing campaigns.

Japan

The contribution from Japan included a background on the extent of the use digital control system and expanding its use recently in fully digitised plants, based on the experience gained over 15 years of operation of these systems. The study reported on their experience with the use of Problem Oriented language (POL), lessons learned from testing and management of digital systems, and a case study involving the failure of a memory element.

Highlights of the experience reported in this study are included in the appropriate sections of this report.

United Kingdom

Reference [6] reports on a research project in the U.K., aimed at gathering operating experience information from a number of plants, including a wide range of industries, on the factors which are believed or observed to have a sensitive influence on software reliability. Those factors which are sensitive would be used to formulate a data collection model relating observed reliability to a set of

parameters characterising the software and its environment. These parameters include measurable quantities (e.g. number of lines of code) or qualitative parameters (e.g. standards applied to the design process). Data collected regarding these parameters has been recorded in a database and used to formulate a reliability model.

Because of difficulties in characterising the software and its environment in general terms in such a way as to make the model generally applicable, it was proposed to restrict consideration to a type of system which uses a limited range of instructions and is used in applications of a similar nature.

Programmable Logic Controllers (PLCs) were identified as a type of system which meets these criteria and therefore offers good potential for the successful characterisation of the code and the environment. They are also very widely used in safety related and non-safety related applications offering a sizeable population for observation.

3. TRENDS AND OBSERVATIONS

The U.S. study [4] found two results. First, electromagnetic interference (EMI), human-machine interface error, and software error caused significant number of digital system failures during the period 1990 through 1993. Fewer failures were caused by random component failures. Second, the NRC reviews digital I&C systems for electromagnetic compatibility (EMC), software reliability, and human-machine interface when it performs a safety evaluation of digital upgrades submitted by a licensee.

Table 1 lists the total number of events by category. The table shows that software errors (30 failures), human-machine interface errors (25 failures), and EMI (15 failures) are the dominating causes of the digital system failure events. However, only 9 events were caused by random component failure.

Table 1. Total number of events by category (U.S.)

Cause of Events	Number of Events
Software error	30
Human-machine interface error	25
Electromagnetic interference	15
Random component failure	9

The evaluation of the U.S. data found that software failures, human-machine interface errors, and EMI caused more than 89 percent of the digital system failure events. The root causes of these failures were (1) poor software V&V, (2) inadequate plant procedures, and (3) inadequate EMC of the digital system for its environment. Most of these failure events did not cause a significant safety event; however, these failures could cause common-mode or cause failure, which can lead to significant safety events.

The AECB study in Canada provided the results shown in Table 2. Based on the analysed data, the following observations were made.

1. Almost all trends, in the investigated failures were either decreasing or they were flat, except for those attributable to inappropriate human actions and jumper-related faults. The data indicate that the incidents of inappropriate human actions has shown a marked increase in the last five years.

2. Software faults are still decreasing, which is an indication of the presence of latent faults left over from development, and not yet discovered.

3. most failures were associated with the Digital Control Computers (DCCs); this is because most of the computer related events deal with DCCs. The DCCs have been in use since the 1970's and perform a complex and continuous task, so that software failures would tend to be more prevalent.

4. The control and shutdown computers are designed to be fault tolerant and, on their own, cause few failures due to hardware. However, the plant hardware associated with the computers is extensive and many events that involve computers are caused by ancillary device failures. Hardware failures should therefore be assessed not only from the point of view of unavailability but also in terms of their impact on the software and the resulting consequences.

5. Software problems are sometimes corrected with a temporary change installed outside the programmable part of the software, often referred to as "patch". Even if put in correctly, the patch appears to cause further problems.

6. Programmable logic controllers (PLCs) are being introduced as a cost-effective method of replacing older analogue or digital controls. PLCs have resulted in a number of incidents within the plants and it must be recognised that they are themselves digital computers. The hardware and software for PLCs should be subjected to the same controls as with the DCC and the shutdown system (SDS) computers.

Table 2. Total records in survey 459

HARDWARE PROBLEMS		**SOFTWARE PROBLEMS**	
Processor	7	Executive/OS	4
Memory	9	Application	103
Interface CCA	31	Database/Table	4
Internal PSU	13	IO Routine	0
Connection	25	Software Other	5
Ancillary	109		
Peripheral	18		
Hardware Other	6		
HUMAN-MACHINE INTERFACE PROBLEMS		**EXTERNAL**	
Inappropriate Human Action	98	External Power	28
Operating Manual	26	EMI	3
Bad Communications	4	Other	8
Procedure Other	2		
UNASSIGNED	37	**MECHANISM OF THE FAILURE**	
COMPUTER SYSTEM		Requirements	19
DCC	364	Design Error	35
SDS1	12	Coding Error	23
SDS2	13	Manufacturing Error	11
SDS - Both	4	Part Failure	124
FM	21	Workmanship	19
SORO	8	Other	19
PLC	13		
Computer - Other	23		
EFFECT ON THE PLANT		**STATUS OF THE PLANT**	
Service Interruption	79	Steady State	286
Service Degraded	126	Transient	5
Inconvenient, not def	73	Maintenance	20
Minor, deferrable	112	Commissioning	13
Safety Related	45	Upgrade	0
Not Specified	23	Run Up	33
CORRECTIVE ACTION TAKEN		Shutdown	38
Replace	130	Offline	4
Redesign	65	Not Specified	55
Restart	15	**JUMPER IN EFFECT**	
Retrain	4	Jumper in effect	25
Revise	72		

The U.K. study on the PLCs reported conclusions based on data gathered from PLC operating experience:

1. From the data collected, the Average Failure Rate of PLC software has been calculated to be:

All faults	2.68 x 10-2/y
Safety Significant	9.85 x 10-3/y
Production Significant	1.43 x 10-2/y

2. Of the faults reported (30 in total), 16.7% were due to errors in the software specification, 46.7% were due to programme design or coding errors and 16.7% arose out of changes made to the software during operation.

3. The relationship between failure rate and various measures of the system size and complexity was investigated. The most significant correlation is between software failure rate and programme size (as measured in the number of relay ladder logic relay coils).

4. The data shows a decreasing failure rate with time of an approximately exponential form. Some of the failures above the generally exponential trend are those due to software or plant modifications several years into the life of the system.

5. The data shows a clear benefit from the use of structured design methods (e.g. Scors, Graphset, Data Flow Diagrams), software support tools and fault identification techniques (e.g. static and dynamic analysis). There is insufficient data to attempt to model the benefits of each technique but the data suggests that such techniques or a combination of them can reduce failure rates by a factor of up to 4.

6. There is a clear negative relationship between failure rate and time under test although there is insufficient data to deduce the form of the relationship.

7. The study would benefit from expansion of the database to cover more systems and it is hoped that further data collection and data exchange with other projects in a similar field will be possible in the future.

France reported in a number of studies the experience with the Controbloc (the PLC in use for the 1300 MW nuclear power plant operation). IPSN carried out a functional study covering the 1985-1993 period for Controbloc system to assess the consequences of incidents on safety. A synthesis of 52 significant incidents submitted by EDF and involving the Controbloc was done. Although the Controbloc reliability in operation was reported as satisfactory, it was assessed that difficulties, encountered by technicians when putting the Controbloc racks back in operation, as well as several spurious signals, might be of safety significance. Consequently, EDF initiated multi phase design review and complementary studies to assess the losses of racks and the consequences of spurious signals.

With regard to the new 1450 MWe units, EDF carried out an I&C system failure analysis (spurious signals or failure to send signals) for the design of single or group of actuators during normal plant operating conditions. This study led EDF to reconsider the distribution of several actuators among control cabinets, for example when the same cabinet controlled a blowdown valve and its associated isolation valve.

4. FAILURE MODES OF COMPUTER-BASED TECHNOLOGIES

4.1 Generic Failure Categories and their Consequences in Safety Systems

Hard failures are permanently damaged parts, where replacements must be installed to restore the system to normal operation. The lethal damage may be due to a broken connection on the microchip in an area smaller than one-tenth the cross section of a human hair, or it may be due to overstress (e.g., from heat, electrostatic discharge, electromagnetic and radio frequence interference EMI/RFI, nonthermal smoke) of several components on a board simultaneously.

Upsets are temporary or intermittent malfunctions that have the potential for causing serious consequential damage. For example, an upset may cause a microprocessor to retrieve instructions that do not correspond to the software written for it to execute. This may cause the microprocessor to output address, data, and status signals that are not defined by the software written for the microprocessor, resulting in a potentially disastrous response of the system.

Failure modes of computer-based systems that may be observed during the operation of a nuclear power plant have been classified by [7] in terms of their generic potential consequences into five categories: (A) critical failures, (B) potentially unsafe failures, conditionally safe failures, (D) latent failures, and (E) fail-safe failures. For the short-term effects, failure category A is considered to be the most serious, while failure category E is the least serious. As explained below, failure categories A and B can result in loss of functionality, that is, loss of the ability of the module, channel, or subsystem to perform its intended function. Failure categories C and D may not necessarily result in loss of functionality, and failure category E will not result in loss of functionality since the implication is that the system is designed to fail safe upon the occurrence of the upset. It is important to recognise that, in a redundant system such as a reactor protection system, an error that leads to any of these failure categories will not necessarily prevent the entire safety system from performing its function, unless there is a common mode failure in two or more redundant channels of the system.

(A) Critical Failure

This is an upset in a component or module that can prevent a safety-related channel from performing its function if and when required to do so. That is, the upset can cause the channel to fail in an unsafe manner. For example, EMI-induced upsets may cause a digital actuation nibble (4-bit) output to give erroneous results.

(B) Potentially Unsafe Failure

This is an upset in a component or module that would likely prevent a channel from performing its function. However, the adverse effect of such an upset can usually be offset in a typical power plant safety system through engineering design. For example, a number of serial and network communication time-outs may occur because of parity and overrun errors. In a safety system, the most serious consequences of such time-outs can be offset by automatically placing the channel in a tripped state.

(C) Conditionally Safe Failure

This is an upset in a component or module that has the potential to prevent a channel from performing its function. However, the affected component or module is able to recover in time for the required function to be performed without exceeding the channel response time requirements. For example, data may have

to be retransmitted on the network on several occasions because of a lack of acknowledgement by the receiver for messages sent. A conditionally safe failure, if it persists, may lead to a potentially unsafe failure.

(D) Latent Failure

This is an upset in a component or module that will typically not prevent a channel from performing its function in the presence of the stressor causing the upset. However, failure may occur at a future date, long after the stressor has been removed. Examples are changes in leakage current, pulse rise and fall times, and other component parameters that nevertheless remain sufficiently within tolerance for the affected channel to perform normally for some limited period of time. For example, it has been reported that one latent failure in a satellite system did not surface for 5 years.

(E) Fail-Safe Failure

This is an upset in a component or module that puts the channel in a tripped or safe state. At the board or system level, however, the effect of upsets includes data errors due to bit changes in memory cells, board failures due to processor lockup, and interface failures (e.g., time-outs on serial interfaces).

4.2 General Failures that are Typical of Distributed Digital Systems

The following examples identify general error categories that are typical of a digital distributed system.

(A) Serial Communication Errors

There are a variety of serial data communication standards and protocols, among the more common of which are RS-232, RS-422, RS-423, and RS-485. Some proposed ALWR (advanced light water reactors) safety system designs will employ either RS-232 or RS-485 data links. Error detection schemes for such data communication technologies are typically limited to the ability to detect single-bit (parity) errors in the data.

(B) Network-Related Errors

As in the case of serial communication systems, many network architectures, protocols, and standards exist. Some network communications are deterministic in nature, which means that every node is guaranteed a fixed time for communication, and control actions must take place in the allotted time. Other network communications are nondeterministic (e.g., Ethernet). For obvious reasons, however, all network communication protocols used within any part of a safety system must be deterministic.

(C) Loss of Data Accuracy

In a traditional analogue safety system, errors may result from process signal drifts from transmitters. In a digital system, another source of error may come from the Analogue-to-Digital (A/D) modules as a function of environmental stressors.

(D) Unintended Digital Actuation Errors

A feature common to most trip systems is that the output leading to actuation units (e.g., solid state relays) is a discrete signal. The digital output to load drivers is arguably one of the more vulnerable parts of a

digital safety system, since its malfunction may either cause a spurious trip of the channel or it may prevent the channel from performing its final actuation function.

(E) Permanent Board Failures

At the system level, many component failures (e.g., damage to a memory cell, processor lockup) may also lead to corrupted data and communication time-outs. However, such manifestations will typically be permanent and will persist even after power-down and restart of the affected node or module.

4.3 Examples of Upsets in Digital Systems

Table 4.1 [7] illustrates generic environmental stressor-induced upsets in digital systems and their potential consequences in terms of the classification scheme mentioned above. The table also lists some specific examples of the generic stressor-induced upsets that were observed during testing.

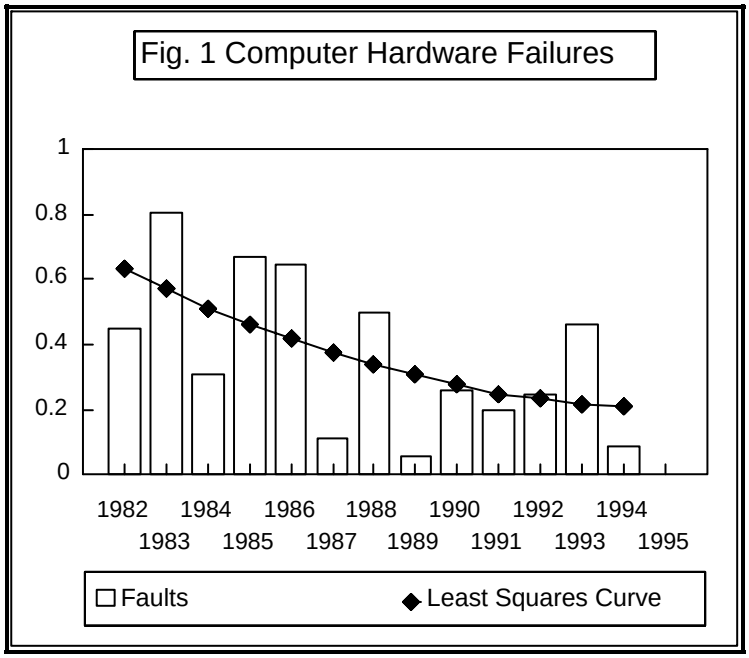
Table 4.1. Generic environmental stressor-induced upsets in digital systems and their potential consequences [7]

Generic stressor-induced errors in digital systems	Some plausible or actual examples observed during testing	Consequence classification
Permanent component/board failures and upsets that lead to unintended and unsafe digital actuation errors.	EMI-induced upset caused digital actuation nibble to give erroneous result.	Critical Failure
Component/module upsets that would usually prevent a channel from performing its function, but whose adverse effect in an actual plant safety system can be offset through engineering design.	Serial and network communication time-outs occurred because of parity and overrun errors.	Potentially Unsafe Failure
Component/module upsets that have the *potential* to prevent a channel from performing its function. However, the affected component or module is able to recover in time for the required function to be performed.	The digital trip computer (DTC) had to retransmit data on the network on several occasions because of a lack of acknowledgement of messages sent.	Conditionally Safe Failure
Component/module upsets that will typically not prevent a channel from performing its function in the presence of the stressor causing the upset. However, failure may occur long after the stressor has been removed.	Changes in leakage currents, noise margins, pulse rise and fall times, and other component parameters that nevertheless remain sufficiently within tolerance for the affected channel to continue to perform normally.	Latent Failure
Component/module upsets that place the safety channel in a tripped state.	Digital nibble output stuck in a "tripped state". (NOTE: this is a plausible example that could have occurred during testing)	Fail-Safe Failure

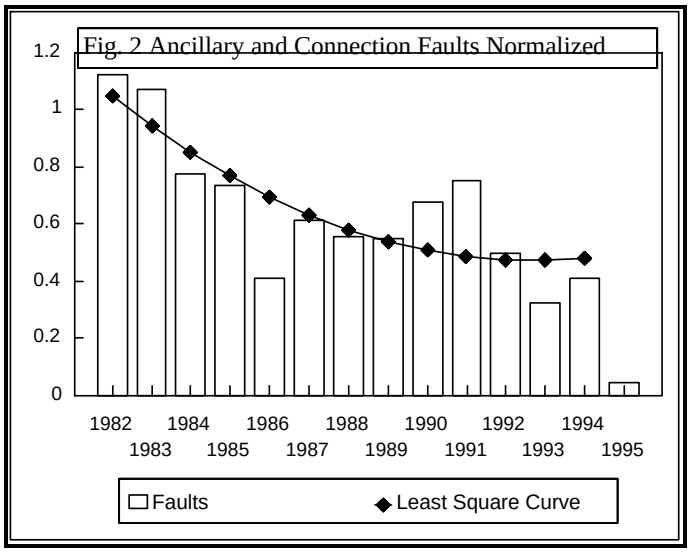
5. COMPUTER HARDWARE AND ANCILLARIES

5.1 Operating Experience

In the Canadian study [5], the computer hardware, consisting of memory, processor, interface circuit cards, internal power supply unit (PSU), and peripherals, shows a lower failure rate relative to other leading categories, most likely because of the design of the equipment, which is fully duplicated and, therefore, is fault tolerant. In other words, a single hardware fault should not affect the operation of the computer system or the plant. It was also found that the number of computer hardware faults has decreased steadily with time (Figure 1).



The most common hardware problem was associated with ancillary devices. This category refers to parts and sensors outside of the computer 'box'. For example, common elements in this category are sensor and relay failures. Given the nature and complexity of some of the sensors used in nuclear power plants, this finding is not unexpected. Even if utilities did not use digital computers, these sensors or their equivalent would still be required to monitor the state of the plant. Ancillary failures showed also a decreasing trend with time (Figure 2).



The second highest failures within the hardware are the faults with the circuit card assemblies (CCAs), connections and peripherals (see Table 2). Problems with CCAs and the decreasing trend of hardware faults over time agrees with the observed experience of the CANDU plant, Wolsong-1, operating in Korea for more than 10 years [8] reported that computer systems encountered a high number of problems in the early stage of operation. Problems arose from oversights in design, manufacturing defects or installation. The majority of failures that have occurred on the control computer systems were attributed to the input-output systems. Bulk Memory System also at Wolsong-1, (Fixed Head Discs) experienced, in the mid 1980"s, major failures and were subsequently replaced with dynamic random access memory units. On a restart, all of the core memory is saved on the disc and a fresh version is transferred to core. The saved data is then used to analyse the cause of the initial stall.

Many of the reported printer failures are caused by mechanical failures. Although printers may be viewed as one of the computer peripherals, their failures could cause computer stalls leading to major reactor transients. A recent event occurred at Bruce-A unit 4, where jamming of a computer printer ribbon caused its buffer to fill and stop the execution of a programme. This caused the control computer to stall and close the cooling flow supply valves to the fuel tube.

The event prompted recommendations for software and hardware changes to ensure cooling flow to the fuel is maintained at all times in case of computer stalls.

5.2 Environmental Conditions

Environmental Stressors

Equipment situated in a control room environment is not affected by a reactor system's design basis events and anticipated abnormal occurrences. Rather, the potential initiating events for equipment stress are from an entirely different set of events. For increasing temperature, the primary initiating event is a loss of heating, ventilating, and air-conditioning (HVAC) systems in the equipment room. For humidity, the initiator could be a water spill or use of water for fire suppression. EMI/RFI sources include walkie-

talkies, welding equipment, or spurious emissions from other electronic equipment. An electrical equipment fire is the primary initiator for smoke

Digital systems have different failure modes and fail at different levels of stress than analogue components. For an analogue system, the effect of temperature rising from 24°C to 49°C (75°F to 120°F) is often merely a loss of calibration accuracy. Digital systems, on the other hand, can suffer more serious effects, including failure to perform their functions at all, because of communication failure or lockup of the central processor. These factors led to identifying elevated temperature, humidity, EMI/RFI, and smoke (e.g. from an electrical fire) as the environmental stressors for digital equipment. Additionally, these stressors have the potential for affecting more than one division of a safety channel and are thereby a potential source of common cause error.

Submergence, elevated pressure, and radiation can be considered physically prevented from occurring in the mild location where the digital equipment is located.

A comparison of the failure types for all the stressors show that more severe errors were encountered during the EMI/RFI tests than during the tests involving other stressors. For example, the EMI tests produced only one permanent failure (i.e., power supply). In addition, during the initiation of one of the smoke tests, EMI/RFI generated by sparking devices used to ignite cables for smoke generation appears to be the cause of a critical failure. The fewest number of failures occurred during the temperature and humidity tests.

At Wolsong-1 (Korea), high failure rate was reported [8] on the integrated circuits of the shutdown computers, for many years. Failures were reduced by providing heat sinks to the IC's, installing air conditioner, and making holes in the cabinet. In addition, alarms were installed to draw the attention of the operators to the high temperature condition.

Electromagnetic Interference (EMI) / Radio Frequency Interference (RFI)

Within the operating environment of the plant, systems my produce random electrical noise known as EMI or RFI. Digital equipment, which operates at higher speeds and lower voltages than the analogue equipment it replaces, is specially vulnerable to EMI. The EMI was the cause of 3 events in the Canadian study and 15 events in the U.S. study. The relatively high number of events in the latter appears to be due to the broader definition of EMI in the U.S. study which includes poor grounding and poor connections.

The ability of equipment to function satisfactorily in its electromagnetic environment without introducing intolerable disturbances to that environment or to other equipment is known as the electromagnetic compatibility (EMC). In reviewing EMC, the US NRC requires a licensee to perform tests and measurements to demonstrate that the replacement digital system is qualified for its environment.

Of the six different EMI/RFI susceptibility tests performed, the system and its interfaces were found to be least susceptible (no errors) to radiated magnetic fields in the range 30 Hz to 30 kHz (RS01 tests). Most of the errors were produced by the conducted spike tests. Errors also occurred with the radiated electric field tests. It should be noted that the relative susceptibility of particular systems can be mitigated by grounding, shielding, isolation, and surge withstand practices.

High-voltage spikes on power leads were found to cause a greater number of upsets and within a relatively short time (i.e., seconds) compared to low-voltage, sinusoidal rms noise on the same power leads. In the latter case, errors did not occur until several minutes into the application of the noise voltage. These results are consistent with expectations, since EMI/RFI-related upsets/failures are typically caused by the

EMI/RFI inducing a high enough voltage to cause malfunctions such as false triggering of digital devices, inadvertent bit changes in memory devices, or breakdown of on-chip protection. If an EMI/RFI burst is going to have an effect via these mechanisms, it is reasonable to expect it to do so in a relatively short time within the application of the EMI/RFI burst.

Elevated Temperature

The different temperature ratings among the various subsystems of the tested digital equipment afforded an opportunity to investigate the effect of temperature/humidity stressors on various I&C subsystems and their interfaces as they approached and exceeded their rated temperature/humidity specifications. Some subsystems experienced temporary failure about 8°C (15°F) or more *below* manufacturers' ratings, while others did not fail even when they were stressed more than 17°C (30°F) above manufacturers' ratings. These observations underscore the need to qualify commercial-grade components despite manufacturers' advertised ratings. There is evidence to suggest that design flaws were responsible for the equipment that failed below manufacturers' rating. Partly because of experience gained from stress tests routinely performed by semiconductor manufacturers, the reliability of current digital components appears to be such that system vulnerability to degraded performance, rather than catastrophic failures, is the likely result of temperature/humidity stresses on microprocessor-based systems in controlled environments. Consideration of these effects during design can address the consequences of these upsets so that fail-safe conditions will result.

Smoke

During testing, subsystems of digital equipment were operated while being subjected to various levels of smoke that approximate credible control room fire scenarios (a control panel fire, a general area fire, and a small in-cabinet fire). The focus was on the performance of the system while under exposure to smoke. This corresponds to the need for safety systems to be functional during a fire, presuming that manual plant shutdown and fire suppression will be the response following discovery of the fire. For these smoke exposure tests, a 1-h exposure was selected as an appropriate test interval. Communication link errors were observed at all levels of smoke density, ranging from a few network retransmissions at low smoke densities to serial communication time-out errors at higher smoke densities.

The severity of the errors generally increased as the smoke concentration increased. Communication errors were observed at all levels of smoke, ranging from network retransmissions at low smoke densities to serial link time-out errors at higher smoke densities. This observed behaviour underscores the potential difficulty of thoroughly ridding a previously exposed board of all residual smoke particulate through cleaning and may point to the need to replace all exposed circuit boards after a fire as a matter of policy.

It is noteworthy that the computers under test exhibited no permanent failures or serious upsets such as processor lockups resulting from smoke particle deposition, although soot was spread throughout each chassis by the computer's fan. On the other hand, the communication interfaces of the fibre-optic modules (FOBs) were found to be vulnerable to smoke deposition when the circuit boards were directly exposed.

Several fire suppression simulations were included in the tests. This included the addition of humidity in the form of steam and CO2 from a fire extinguisher. The results of the humidity (85% RH) tests showed that humidity may be an important factor in creating temporary shorts, and its adverse effect on digital boards is likely to increase with the severity of the smoke exposure. The CO2 had very little effect on the equipment, although the temperature in the chamber dropped drastically.

Stressor Intercomparisons

While the nature of environmental tests does not permit a rigorous statistical comparison of the effects of the various stressors, the authors of [12] have attempted to make a conservative comparison by making some assumptions. Their results show that EMI/RFI upsets had the most severe effect on the equipment, followed by smoke exposure and then elevated temperature at high relative humidity.

Reliability of Data Communications

It was observed that a significant fraction of all errors resulting from the application of stressors is communication errors. Many of these errors were time-out errors or corrupted transmissions, indicating failure of a computer to receive data from an associated multiplexer, optical serial link, or network node.

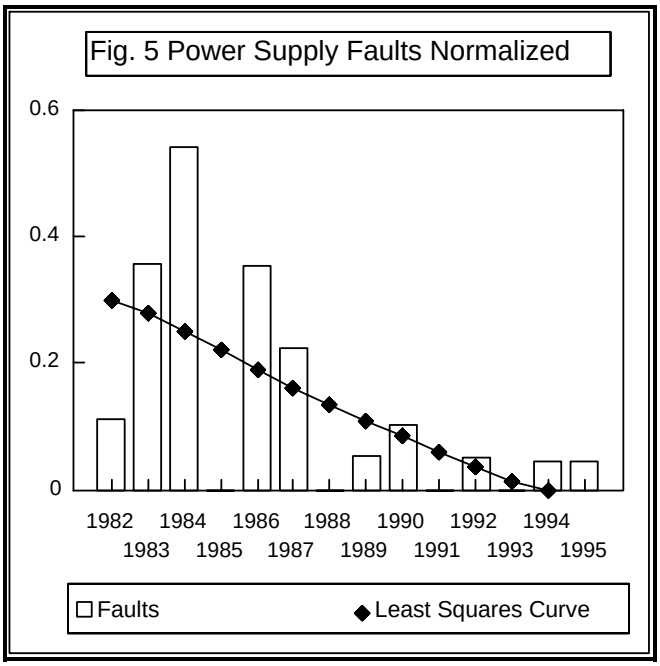
A method of improving the reliability of data communications is to use data redundancy. This simply involves adding some redundancy to the data bits, which is then used to check the validity of the data every time the latter is referenced. For low error rates and small memory applications (below 1 MB), parity checking is a good choice. A parity error indicates data corruption but is limited to the detection of only single-bit errors. The more sophisticated Hamming code can detect two-bit errors and correct one-bit error in a word. Hamming code-based error detection and correction technologies are well suited to moderately noisy systems, which includes microprocessor-based systems with more than 4 MB of main memory

5.3 Aging and Seismic Qualification

Aging does not appear to pose a significant design concern for digital systems because the equipment is installed in a mild environment and because it is accessible for monitoring, calibration, and replacement. Consequently, the equipment can be expected to be serviced or replaced as necessary throughout the plant life. The installed equipment can thus be assumed to have like-new performance.

Seismic qualification of digital components does not appear to pose any unique qualification issues. Surface-mounted integrated components are recognised as rugged components and are routinely used in applications such as automobiles, aircraft, and portable electronic equipment in which accelerations typically exceed that of a design basis earthquake.

5.4 External Power Supply



The Canadian study has shown that problems with external power supplies represent a not insignificant number of failures, despite the fact that power supplies are designed to be fully duplicated and uninterruptable. However they decreased with time as deficiencies were removed from the systems (Figure 5).

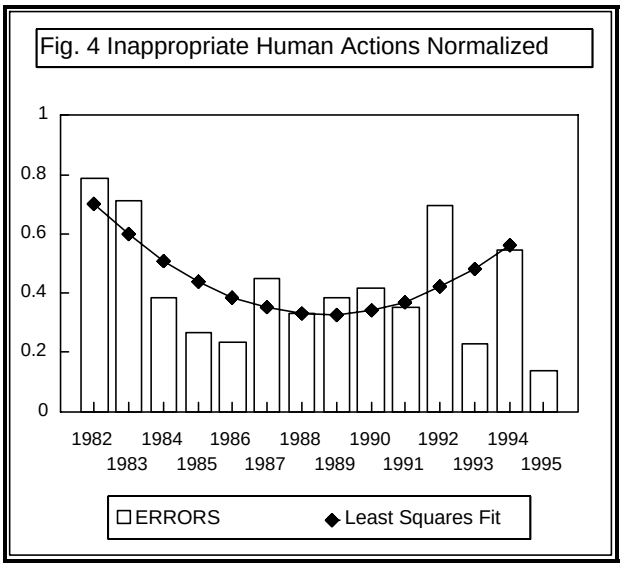
5.5 Human Machine Interface

The definition adopted in the U.S. study [4] states that human-Machine Interface includes all interfaces between the digital system and plant personnel, including:

- Operators - alarms, status displays, and control interfaces.
- Maintenance technicians - test and calibrations interface, diagnostic information displays, and data entry terminals for setpoints.
- Engineering personnel - configuration workstations and terminals

Human-machine interfaces also include unauthorised computer data entry, deviation from procedures, and inadequate procedures from plant personnel. For the purpose of presenting observations in this report from different participants in this study, this broad definition will be adopted.

Both the U.S. study and the Canadian study indicate that the inappropriate human actions contributed to about 25% of the computer-based system events. Preliminary results from the Canadian study indicate an increase of these events in the last five years (Figure 4)



The French study provided a number of lessons learned from IPSN experience in evaluating a recently installed computer-based monitoring and control (KIC) system for use in the control room of units B1 and B2 at Chooz NPP. The following is the main lessons learned during the final phase of the pre-installation ergonomic testing performed in 1994 using a full scope training simulator:

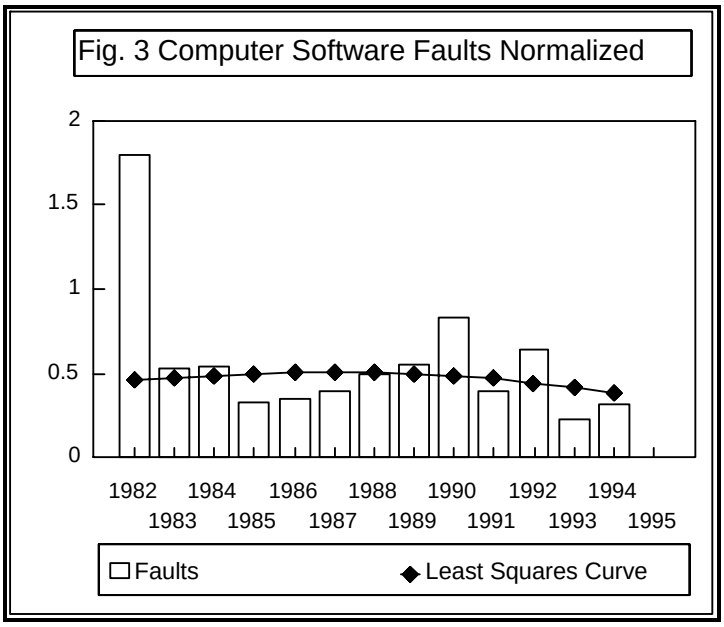
1. The organisation of the crews, validated on previous plants with a non computerised control room, cannot be transferred to a computerised control room without specific analysis of functions of each crew member. This may include, for example, the redundancy and the technical support provided by the supervisor in a computerised control room, during transient and accident conditions. Further studies have therefore been conducted on these aspects.

2. The high level of guidance, provided to the operator by the KIC system, had some peripheral effects on the operator. For example, operators were inclined to follow the instructions and could be too much trustful in the KIC system. Differences were also noted between the logic in the KIC system and the operator's logic. Further studies have therefore been conducted on these effects.

3. The process of simulation does not permit full analysis of the impact of the computerised control room on the crews. Specific observations on site need to be made after the fuelling of the reactor. Further studies have therefore been conducted to define methods for collecting specific data, from feedback, relevant to human machine interface.

6. COMPUTER SOFTWARE

The Canadian study [5] reported that software faults represent a significant number of failures. The number of computer software faults has been decreasing slightly with time. A larger decrease in the number of failures can be expected in this area (Figure 3), because once the fault is rectified, it is permanently rectified , i.e. it should not experience wear-out trends.



The U.S. study [4] categorised any event caused by software failure as a software error. Each software error was further categorised as either (1) a software verification and validation (V&V) failure or (2) a configuration control error. Configuration control is the process by which changes to the products of software development are controlled, including the configuration baseline.

The U.S. study found that software errors is the largest failure type among computer-based system failures (Table 1). Failures in the software V&V process caused most of the software error events. A similar observation is made in the Canadian study. Table 2 shows that failures corresponding to the V&V failures, which were further broken down into categories such as "requirement", "coding error" and "design error", represent a high percentage of the software failures.

The Japanese study reported that a good practice was to keep the safety-related system logic simple. To further avoid complex software operation, the use of interrupts was prohibited. Adopting this approach did not result in any complexity. Aside from some small number of errors experienced on site, they have never experienced software errors.

The U.K. study [6] sought a correlation between software failure rate and a number of parameters related to the size and complexity of the software. The effect of each parameter is examined below.

Figure 3.1 - Relationship between Failure Rate and the Number of Inputs

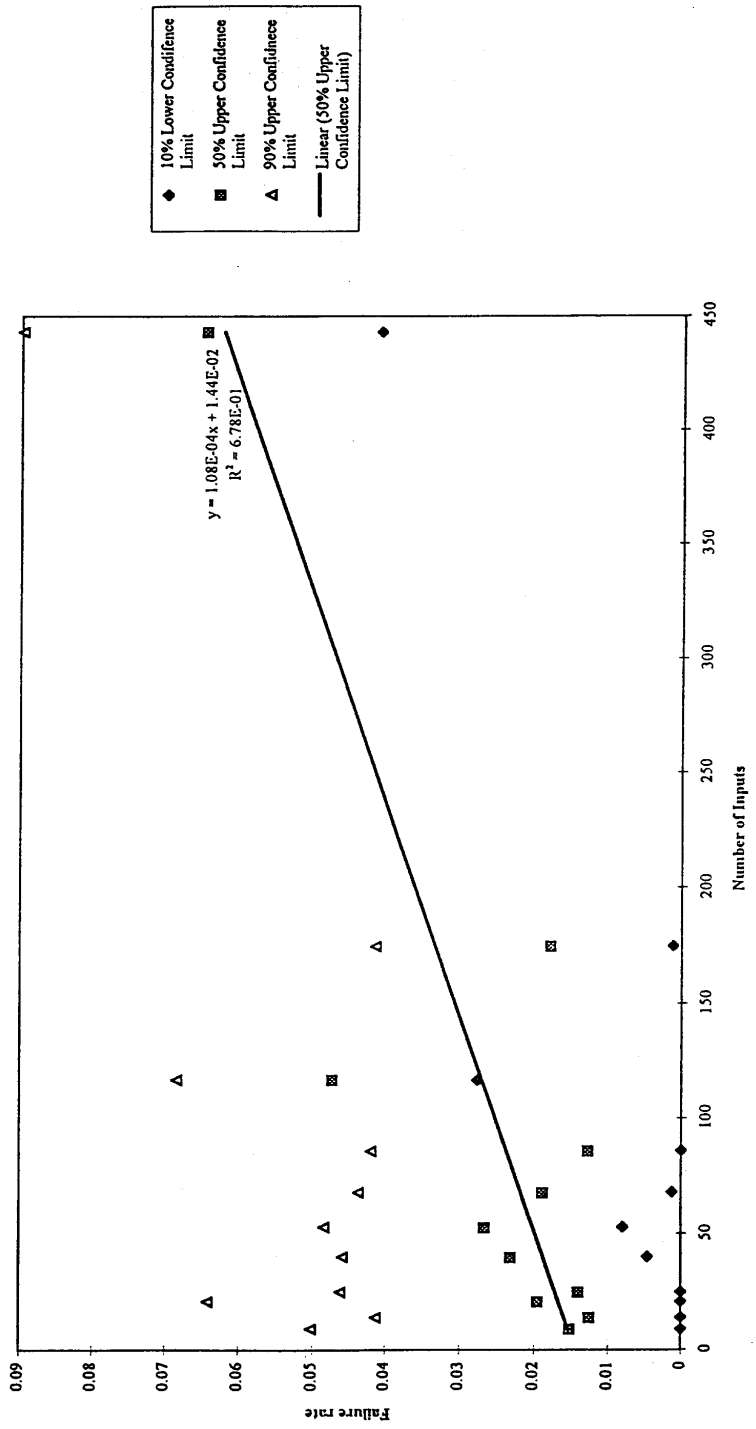


Figure 3.2 - Relationship between Failure Rate and the Number of Outputs

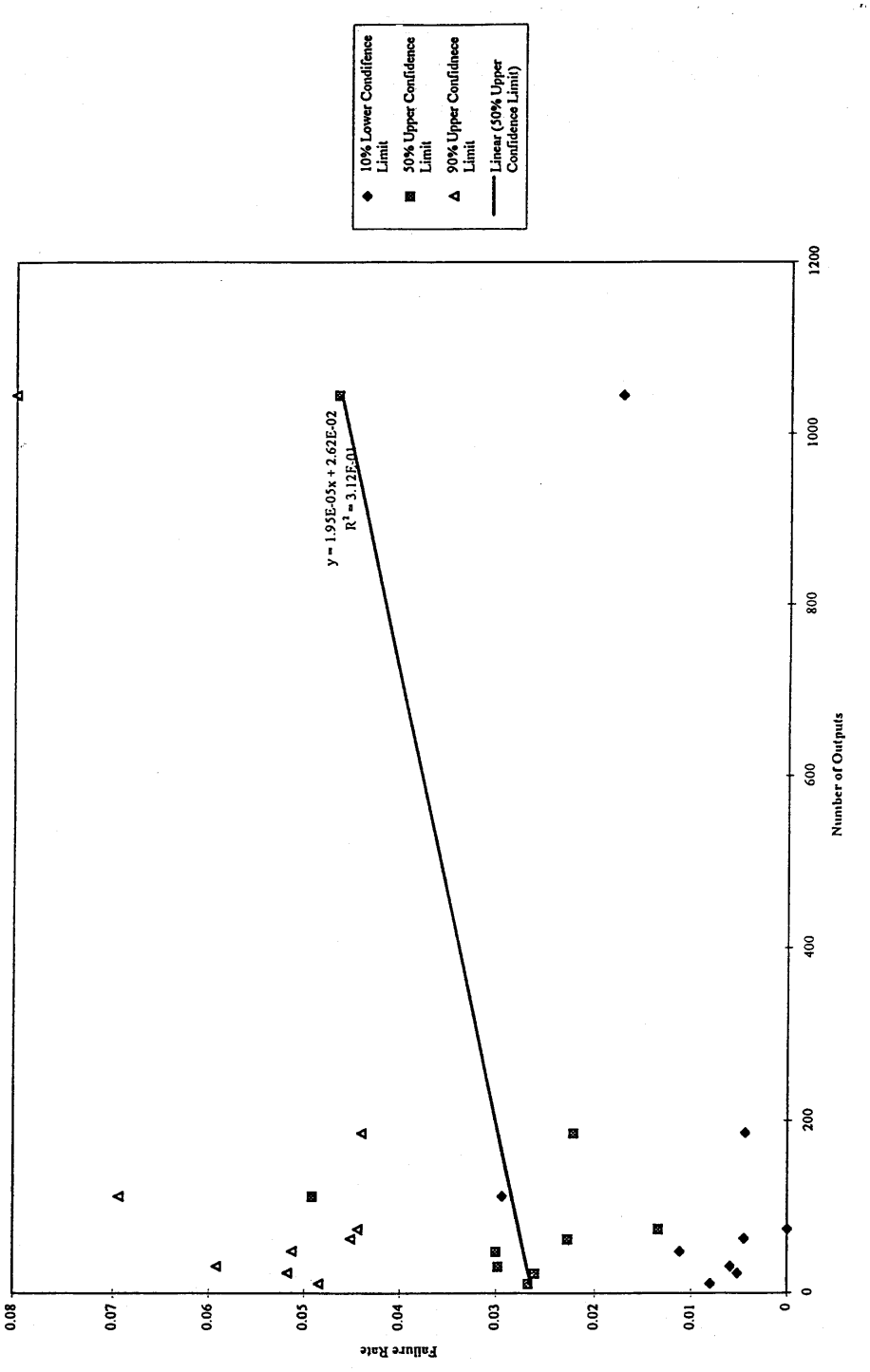


Figure3.3 - Relationship between Failure Rate and the Number of Inputs and Outputs

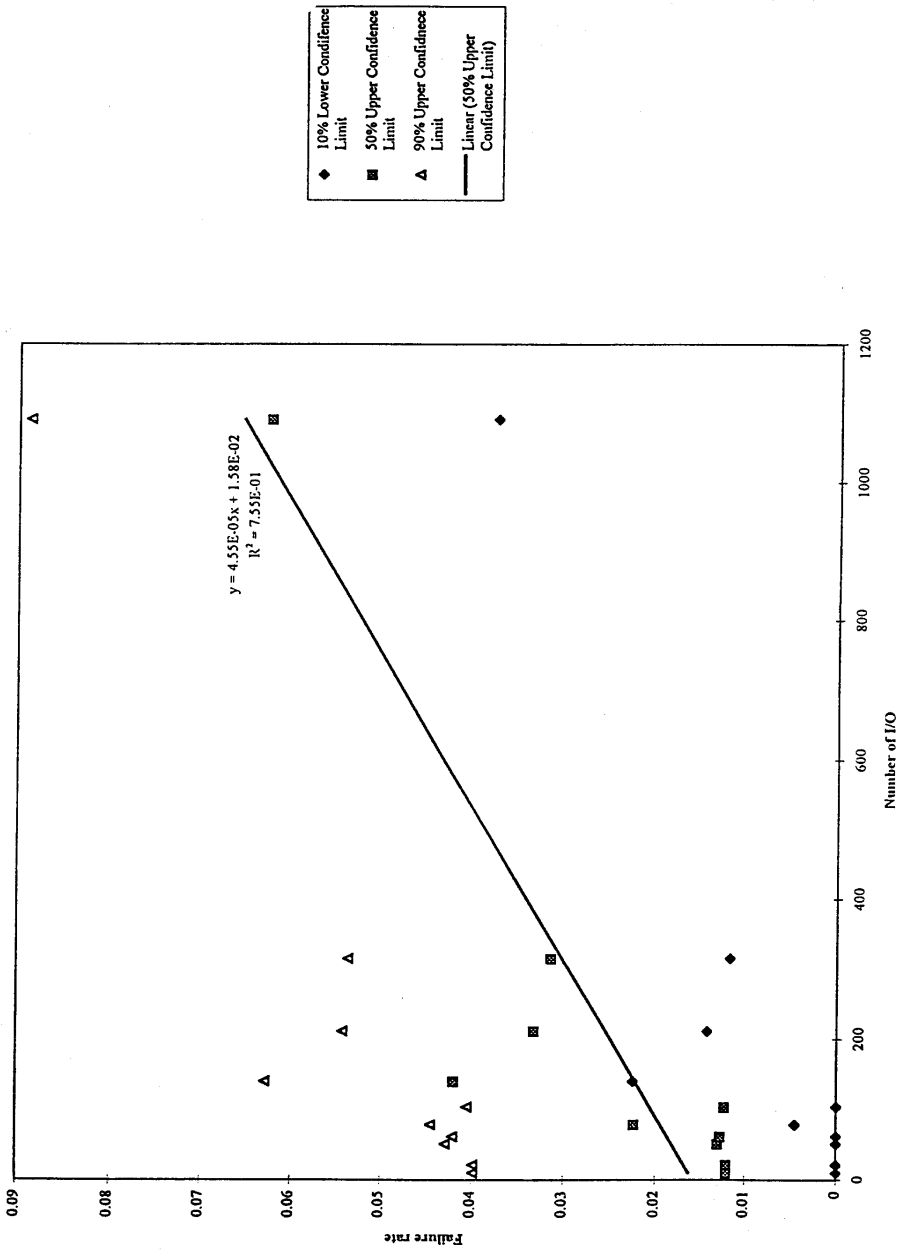


Figure 3.4 - Relationship between Failure Rate and the Number of Coils

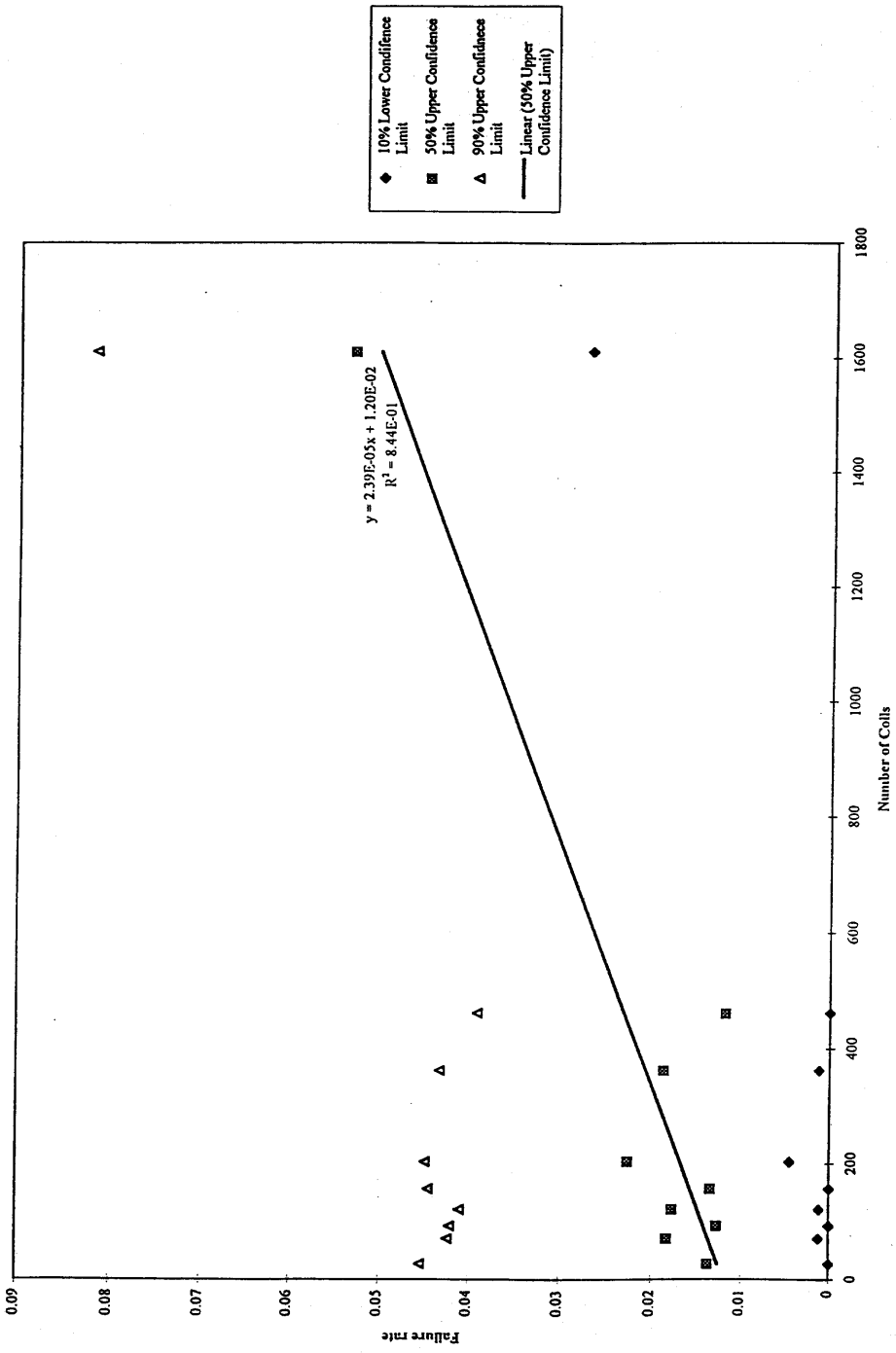
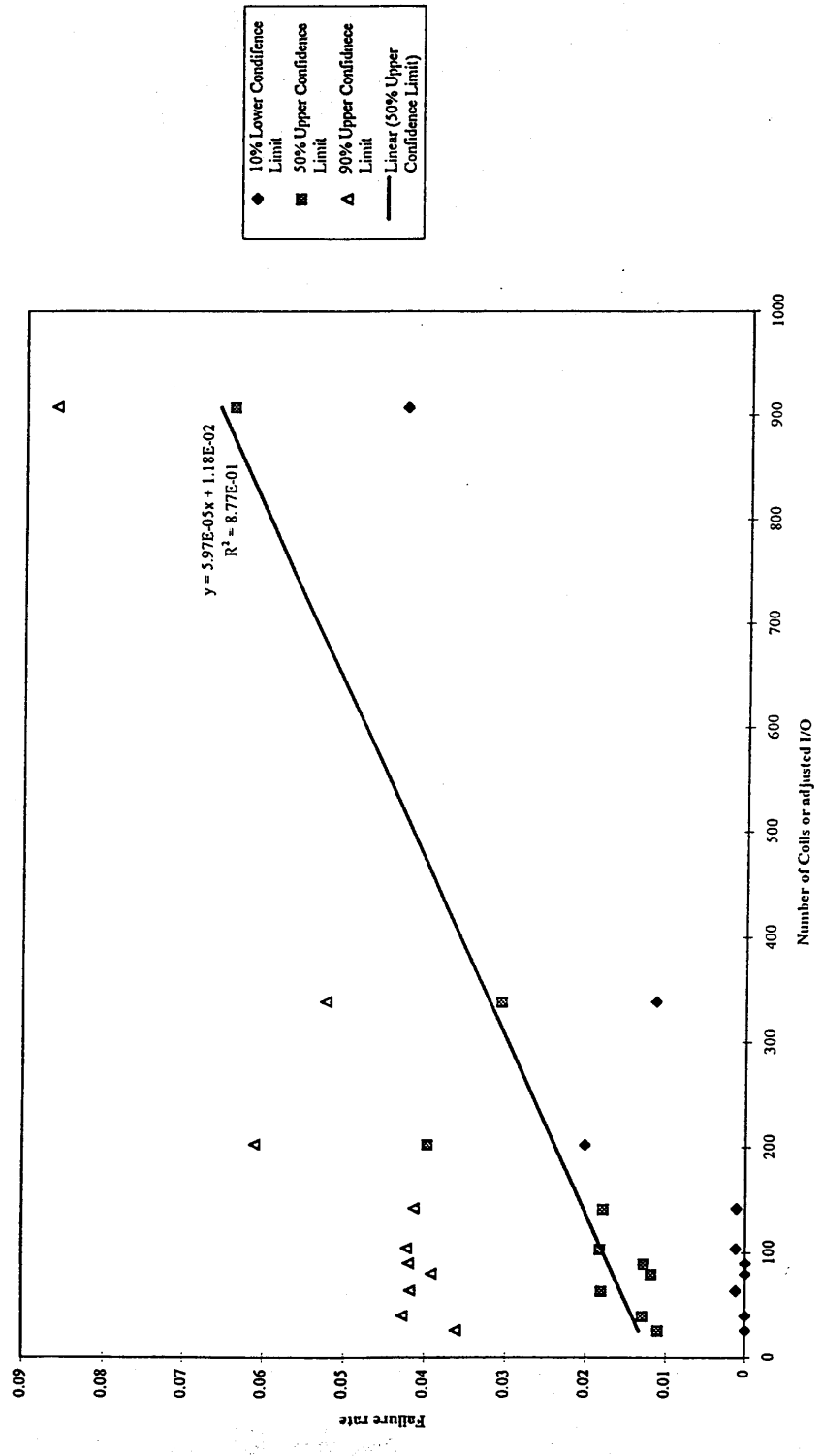


Figure 3.5 - Relationship between Failure Rate and the Number of Coils or Adjusted I/O



Number of Inputs

Figure 3.1 shows the relationship between failure rate and the number of inputs. It can be seen that there is a generally increasing trend but a fairly wide spread of data points from the trend line. The R^2 value is 0.678.

Number of Outputs

Figure 3.2 shows the relationship between failure rate and number of outputs. Although the trend line shows a gradually increasing trend, the fit is poor (R^2=0.312).

Number of Inputs and Outputs

Figure 3.3 plots failure rate against the sum of inputs and outputs. Again, there is a clearly increasing trend but with a fit better than that of Figures 5.1 and 5.2 (R^2=0.755).

Programme Size

Because of the variety of PLC programming techniques, the data collected provided the programme size in a number of ways:

- Number of lines of source code
- Number of ladder logic relay coils
- Number of terminated logic lines
- Number of bytes of programme in memory

The majority of the data collected recorded programme size in terms of the number of ladder logic relay coils. For these systems, the relationship between failure rate and programme size is shown in Figure 3.4.

It can be seen that the straight line fit is fairly good (R^2 = 0.844). However, the graph is dominated by data points at the smaller end and the slope would be very sensitive to the position of the single data point at 1600 coils.

Number of Coils or Adjusted I/O

The best straight line fits are shown by Figures 3.3 and 3.4. Figure 3.4 is, however, based on the subset of data for which information on programme size is available in terms of relay coils.

It was noted from the data that, not unexpectedly, the number of coils was related to the number of I/O. It was calculated that the ratio with the smallest standard deviation was that between the number of coils and the total number of I/O. This relationship was 1.436 coils per I/O (standard deviation = 1.352).

In order to provide additional data, for the systems for which programme size was measured in some way other than by coils, an estimate of the equivalent number of coils was made from the total I/O count and the above average ratio. The results are shown in Figure 3.5.

It can bee seen from Figure 3.5 that there is an improved straight line fit to the data over that using either the I/O count alone or the number of coils alone ($R^2 = 0.877$).

The U.K. study concluded that the best model which relates the software failure rate to a measurement of size or complexity is that resulting from the use of programme size as measured by the number of relay ladder logic coils or, where this measure is not available, by the total I/O count.

A possible interpretation of the model is that there is a part of the failure rate independent of the system size arising from, for example, specification errors due to a misunderstanding of the plant or the requirements, and a part which is proportional to the system size (e.g. logic errors).

7. MAINTENANCE EXPERIENCE

Maintainability of computer-based systems depends largely on the quality factors of traceability, completeness, consistency, simplicity, modularity and testability. The maintainer needs to be able to fully understand the software before it can be changed. Improving upon the deficient quality factors is required in order to improve maintainability. Experience and lessons learned in improving these quality factors through the adherence to standards, implementing modifications, or improving documentation are discussed below.

7.1 Adherence to Standards

A recent rehabilitation programme, described in [9], recognised the need for the software to conform to more stringent software quality assurance standards. The Canadian approach used in the reactor rehabilitation programme, to achieve this, is to use the new Ontario Hydro/AECL Software Engineering standards (OASES). This is a family of standards where each individual standard correspond to a defined level of nuclear safety. For example Category II is used for safety related software such as the Digital Control Computers (DDCs) software changes and the category III standard is used for the Plant Display Systems (PDS) and Safety System Monitoring Computers (SSMC) design. In complying with the standards the utility found the following problems:

- It makes the up-front cost appears to be higher and the development duration longer.
- In attempting to categorise software, guidelines were found to be subject to interpretation; different people may reach different conclusions.
- More and better knowledge of plant operation is required in order to apply the guidelines than what most computer staff possess.

In Japan, maintenance of digital systems is carried out following the same maintenance programme as the analogue system, adding to it the software check. Maintenance of the digital devices, for example, include input/output signal check and memory check involving software comparison with the master programme. Since digital devices are equipped with self diagnosis capability and redundant channels, the errors would be detected immediately even if they emerged during the plant operation. Due to this type of preventative maintenance there were no trouble or failures found during periodic maintenance.

7.2 Strategy for maintaining or replacing

Decisions taken by the utilities on whether to maintain or replace components or systems are based on the operating experience throughout the life of the plant. When opting for replacement, two problems may arise, which could impact on the quality of the procedures:

- Off-the-shelve products my not be fully adequate, which results in complicated procedures. This is in contrast to previous computer projects, where automated tools were not used, but the procedures were much more straight forward.
- Computer hardware and software life cycles are becoming increasingly shorter, in the order of 2-3 years. This creates a problem for maintainers since they have to follow a methodical and slow process.

7.3 Procedures for Modifications

Configuration control has been widely recognised and identified as a crucial area. In France the safety assessment for the N4 computer-based systems considered the general modification process (development and V&V) put into practice by EDF and its suppliers before fuel load as well as specific rules which must be put in place to control modifications after fuel loading (impact analysis and procedures for on-line modifications). The aim is to make sure that each change (be it error correction or evolution to specification) is carried out properly avoiding unnecessary destabilisation and the risk of regression. In order to maintain confidence in the updated version, the adequacy of the requalification should be justifiable. This is particularly relevant when the possibilities for on-line testing are reduced once the reactor has gone critical.

IPSN recommended a formal impact analysis procedure which the licensee implemented. Each modification is considered on a case by case basis by a panel with diverse and independent interests (programmer, operator, etc.). The impact of the correction or not for each error or modification request is considered and supported from the points of view of safety, functionality, operator nuisance, probability of occurrence, diagnosis, implementation and validation. There are categorisations made concerning the gravity of a non corrected anomaly and an attempt to quantify globally the impact of corrections made to a new version by indicating the number of software modules altered. A summary of the impact analysis is presented to the safety authority. IPSN considers it important to have a rigorous approach which is accountable and visible to the safety authority. The onus is on the licensee to make it work.

In France, during the safety assessment phase [1], the process for modification management has been relevant to pre fuel-load. Once the reactor is loaded and has gone critical, the implications of any modification are evidently to be taken very seriously. In the first instance, it is clearly the aim of everyone concerned that the I&C will be sufficiently validated and proven such that modifications will not be necessary between periods of reactor shutdown and fuel unload. However, to be realistic and cover all contingencies, a procedure for safe reinstallation of software has been prepared specifically for the KIC. The safety case relies ultimately on the ability to operate the reactor safely from the diversified back-up panel. There is also the possibility to reinstall a known proven version if ever a modification does not work out.

Although an update of the software is not normally envisaged during reactor operation, the plant configuration data, the "programmable" part of the system, is designed to be modified on line. This is

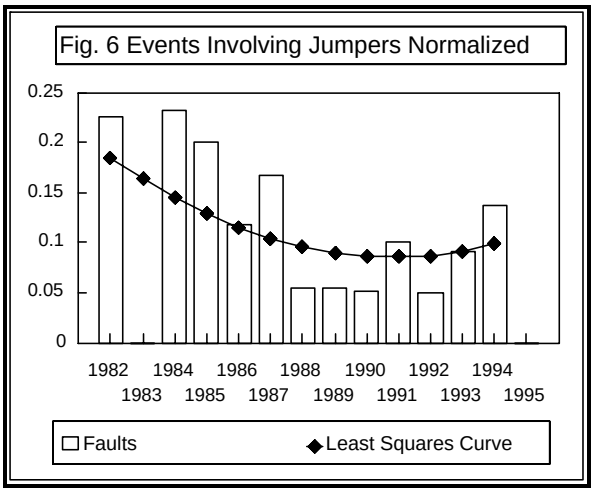
considered as a function of the system and as such has necessitated a particular effort for validation to ensure the absence of interaction between data and system.

The validation of data changes are carried out upstream in the CAD. However, the conditions for data modification during the reactor operation must be subject to prior function analysis to identify plant availability and define special operating conditions. A dry run must be carried out on an off-line configuration before each data modification.

In Japan, when implementing a change in a computer programme, a copy of the stored master programme is revised and verified through the simulation test at the software factory in order to assure the correctness and completeness. After a series of test in the factory, the revised programme is brought to the site and loaded in the corresponding system. Finally the revised programme is tested within the corresponding system.

The impact of modifications on the feed back of operating and maintenance experience was identified in the French study. The cumulative operating experience feedback over the longer term is effectively interrupted for the KIC system software (or any other software) each time a major modification is made to the software. This interruption occurs despite the fact that these modifications are strictly controlled and well documented

7.4 Patching



The Canadian study [5] examined the difficulties encountered with temporary modifications to the software known as "Patching" which is a modification to the software performed outside the programme, e.g. to a data table, that causes the bypass of a sequence performed by the programme. Because patches are temporary; their installation and removal is controlled by administrative procedures using a record known as a "jumper". A recent serious reactor incident at Bruce-A, in 1992 [IRS report No. 1360.00] highlighted the risk associated with patching and with the inadequate control of the software "patching" practice. In this incident, the patch was installed to force the software to operate correctly at a very low reactor power as some power sensors become irrational during reactor start-up. Because the patch was not removed when the reactor power increased the software operated incorrectly and caused a power excursion that was terminated by a reactor trip.

The number of events which involved temporary software modifications or 'jumpers' was found to decline until the late 1980s, but these are now on the increase (Figure 6). Care should be taken in drawing conclusions in this area, because of the relatively small number of failures in some years, and the random pattern of the faults.

7.5 Human and Organisational Factors

The use of human factors engineering (HFE) Principles are becoming increasingly important in the software design and upgrade processes. Utilities in Canada incorporate the HFE programme and also solicit significant input for the new operator interface from the operating staff. An example of this is the process used for capturing the plant display system (PDS) design requirements by directly involving operators.

In France, involving future user staff in certain design tasks is also viewed by EDF as necessary [10]. Users would be part of a team that writes the operating data, design images and charts, proposes computing algorithm or prepare training documents.

7.6 Design Authority and Staff Qualification

Production pressure may cause the utilities to rely on the expertise of their local technical staff in the plant, rather than the original designer or the design authority, to modify the software. The design authority is the entity responsible for recommending changes to the design and maintaining historical records of the design changes and the subsequent verification and testing activities. A dedicated and appropriately qualified staff should facilitate the traceability of changes and minimise the likelihood of software errors.

7.7 Testing the Upgrades

Experience has shown that, following software changes, formal testing should be performed in adherence to stringent standards, similar to the standards required in the development phase. These tests should be as automated as possible. The test procedures should be written such that the specific steps to be done by the tester and the expected results are completely documented. One of the root causes of the incident which occurred at Bruce-A in 1990 [IRS No. 1118.00] (see summary of the event in case study 2), involving unintended movement of the fuelling machine while it was attached to the reactor face, was that the software error was not evident during testing.

Another important aspect is the development of test facilities [9]. Although development tools are very important, maintenance staff believe that testing tools have often not been given sufficient attention on many computer upgrade projects. One plant reported the development of a process I/O emulator and plant simulator (IOES) testing tool for the project.

The French study highlighted the importance of effective use of test results in their KIC project and the problems that can arise from the delay in producing the results. The simulator tests were performed somewhat late when compared to the overall progress of the KIC project. The KIC system software installation had already begun in preparation for the in-service trials by the time the results from the pre-installation ergonomic testing phase were published. The introduction of late modifications and their validation can be very difficult.

The Japanese study indicated that tests were carried out not only to the digital system alone, but also to confirm its response as part of the plant system. For example, plant transients and design basis events such as LOCA, steam line breaks, etc. were simulated to verify the performance of the digital system as part of the plant system. As well, functional tests, performed as part of the periodical maintenance of digital I&C system, should be performed in the same manner in which the installation test was performed.

7.8 Documentation

In contemplating major software changes, compliance with modern standards may make the volume and effort of documentation appear far greater than expected. However, maintenance experience indicated that adequate documentation is essential in reliably performing changes to the software and in performing thorough evaluation [11]. Because modern software standards were not in common use in the mid-1970's there were no software requirements listed in the currently used software which was installed then. The software requirements should specify what the software is functionally required to do and these software requirements form the basis from which thorough tests can be designed. The software requirements are also needed for assessing software quality through measures such as traceability and testability. Other information which was found necessary to perform changes was the description of interfaces between hardware and software, such as where certain inputs can be read by the software. Examples of inadequate software design documentation are:

- no revision number,
- variable listed as coming from the wrong routine,
- a routine does not list any outputs but it was found that another routine indicates that it gets a signal from it,
- a symbol is not listed as being used when in fact it is used for control purpose,
- routines not described,
- a function which has been removed long ago is still described in the design documentation, or
- documentation describing the overall software design and interactions of control programmes are not up-to-date.

Without up-to-date documentation, the process of configuration control may be managed mainly through the skill and experience of the technical staff. This could also cause testing to be done in an ad hoc manner, often relying on the tester to know how to stimulate the software programme and what responses to expect. Following the implementation of the change it is equally important that the step-by-step test procedures and the expected responses be documented. It was also recommended that event reports should be made traceable, i.e., any changes made to the software which are the result of a problem identified in an event report should reference the event report number and that the event follow-up report should reference the software change.

When the decision is made to maintain obsolete equipment rather than replacing it, it was found that the success of maintenance was attributed to the availability of good documentation. At the CANDU plant KANUPP documentation proved invaluable in performing maintenance, despite the presence of new staff [12].

8. REGULATORY EVALUATION

The NRC reviews EMC, software reliability, and human-machine interface issues when it performs a safety evaluation on each digital upgrade submitted by a licensee. The NRC evaluated the licensee's proposal to replace 7100 analogue process protection system with a computer-based digital process protection system. The digital issues that the NRC staff reviewed for its safety evaluation included the reliability of software and EMC of the system and training for human-machine interface. The staff stated that it took the following steps to review the reliability of the software:

1. Performed a detailed review of the system design process and software V&V programme.

2. Reviewed available information on the software and hardware history including previous software and hardware failures.

3. Reviewed the specific plant application, including any special features that were required.

4. Reviewed the V&V performed on the software used in the licensee application. This detailed review included:

   - following the code development
   - examining the vendor/licensee interface and response process
   - reviewing software problem and error reports and resulting corrections
   - comparing the V&V to ANSI/IEEE-ANS-7-4.3.2.-1982
   - interviewing personnel involved in the process
   - verifying the independence of the software verifiers
   - reviewing the development of the fractional requirements and subsequent software development documents
   - reviewing the software life-cycle and future vendor/licensee interface
   - reviewing the V&V results

5. Performed a "thread audit", which consisted of picking a sample of plant parameters and tracing the manner in which the licensee used these parameters in writing the purchase specifications and functional requirements for the software and in writing and testing the codes.

At the end of the review, the staff collected all of the information to establish a benchmark for assessing the performance and reliability of the software safety system.

In the SER, the staff described its review of the EMI qualification in the following sequence:

1. Evaluated the plant environment to find potential EMI sources, including the effect of open doors during surveillance, the types and strengths of plant radios, the location and direction of microwave sources, and the location and effect of other equipment within and immediately surrounding the installed location.

2. Reviewed and evaluated the vendor test methodology, frequency susceptibilities based on the vendor tests, and vendor system modifications to compensate for these susceptibilities. This review included comparing the as-tested and as-installed configuration.

3. Reviewed the licensee's on site testing and analysis.

4. Assessed the system EMI qualification based on all of the above mentioned reviews and evaluations.

The NRC completed its evaluation by considering the licensee's training and procedures. The SER states that an important part of assimilating the computer-based digital process protection system into the station environment is ensuring that all procedures affected by the modification are correctly updated and that the operators and technicians have sufficient training in the use and repair of the new system. The documents reviewed to address this issue included surveillance, channel calibration, annunciator response, abnormal operating procedures, and administrative procedures for plant modifications. The licensee also committed to incorporate into its procedures the detailed operation and maintenance manual received from its vendor.

9. FEEDBACK OF OPERATING EXPERIENCE

For the engineering of computer-based systems to mature, it is important to capture and learn from the experience of using such systems. For example, the operating experience was reported by Japan to have been used in improving control devices in Kashiwazaki Kariwa units 6 and 7 and in expanding these applications to safety protection system.

First, this experience feedback can benefit the design of new systems, allowing the designers to concentrate their efforts on aspects of the design known to have problems such as requirements definition. Furthermore, the information collected on operational experience in the use of COTS software systems is also very useful for the design of architecture that use these systems, especially for the validation of COTS systems. To achieve efficient validation of the global system, the quality and relevance of data is essential. Finally, experience feedback is the basis for improvement to systems currently running in the plants.

To be efficient, the collection of data must be formalised. The systematic study of the Licensee Event Reports (LERs) or significant incidents involving computer-based systems could provide valuable lessons. Current reporting techniques need to be improved to take into account some of the special characteristics of computer-based systems. These characteristics include the digital, on-off nature of computers, and the way their complex logic can obscure the connection between cause and effect. It is also important to understand the relationship between operators and computers so that this interface can be improved and the chance of errors reduced.

A system for collecting operating experience should be problem-oriented and very easy and convenient for operators to use. Any instance of a computer-based system operating in an unexpected or undesired manner should be reported. This may not be directly linked to "significant events" as currently defined. There should be a clear separation between reporting a problem and identifying a cause or a remedy. In general, operators should be asked to report the facts without interpretation, but they can be encouraged to "blame the machine" rather than ascribing a problem to "human error". The report should include:

- information about the environmental conditions, even if they are not seen important at the time of the failure,
- the operating conditions of the equipment and plant,
- an indication of the last intervention made by the maintenance staff on the system.

It is important to coordinate the collection of operating experience with other users outside the nuclear industry. Computer-based systems are adaptable to many applications and industry; no single industry can claim to be unique. The reporting system should assist in identifying similarities between applications and problems.

A reporting system should also be oriented towards collecting as much information as possible without prejudice. Minor problems that do not lead to immediate serious failures could become important in combination with other problems. The identification of a computer system problem may even occur after the event, when analysis is done. Having a historical record of such problems will help in understanding and fixing the system. The problem reports should also be closely tied with the management of system configuration. Computer-based systems generally undergo many changes and adaptations (especially to the software) so it is important to understand exactly which version and configuration was operating when a problem occurred.

10. CONCLUSIONS AND REMARKS

1. Feedback of operating and maintenance experience is recognised as an important input to failure analysis associated with complex systems such as computer-based systems. The process of feedback would provide designers with information on systems failures, unforeseen scenarios, or unanalysed configurations. Following plant start-up, the use of the operating experience have led to reconfiguration of system components. Several views on ways in which this feedback can be achieved have been presented in Chapter 9.

2. Safety Assessments by regulators use the operating experience in a assessing computer- based safety performance prior to installation in areas such as electromagnetic interference, software reliability or human-machine interface. Assessments were also extended to management of modifications after plant start-up.

3. Programmable Logic Controllers (PLCs) appear to offer good potential for successful characterisation of software performance due to their widespread use in safety and non- safety related applications within and outside the nuclear industry. They can provide a sizeable population for observation.

4. While computer-based system failures cause few significant safety events, they could cause common cause failures leading up to significant events.

5. Software modification during operation is one of the major sources for software errors. Maintenance experience indicates that adequate documentation is essential in reliably performing changes in the software.

6. Preventative maintenance concept extends to computer-based systems in different ways, such as the inclusion of self diagnostic capabilities or saving memory data on restart to analyse the cause of an initial stall.

7. Computer equipment situated in a control room are more likely to be affected by environmental stressors than by design basis events. Primary initiating events could be loss of heating, ventilating, and air conditioning, water spills, or use of fire suppression water. While rising temperature, for an analogue system, causes a loss of calibration accuracy, it can cause more serious effects on digital equipment including failure to perform their function at all. More severe errors were found to be caused by EMI/RFI.

8. A significant fraction of all errors resulting from the application of environmental stressors is communication errors. Many of these errors were time-out errors or corrupted transmissions, indicating failure of a computer to receive data from an associated multiplexer, optical serial link, or network node.

9. Aging does not appear to pose a significant design concern for digital systems because the equipment is installed in a mild environment and because it is accessible for monitoring, calibration, and replacement. Consequently, the equipment can be expected to be serviced or replaced as necessary throughout the plant life. The installed equipment can thus be assumed to have like-new performance.

   Seismic qualification of digital components does not appear to pose any unique qualification issues. Surface-mounted integrated components are recognised as rugged components and are routinely used in applications such as automobiles, aircraft, and portable electronic equipment in which accelerations typically exceed that of a design basis earthquake.

10. Software errors constitute a significant number of failures of software. They may include coding error, design error or V&V error

11. Maintainability of computer-based systems depends largely on the quality factors of traceability, completeness, consistency, simplicity, modularity and testability. The maintainer needs to be able to fully understand the software before it can be changed. Improving upon the deficient quality factors is required in order to improve maintainability.

12. Regulatory assessments of digital upgrades focus on issues related to reliability of software, electromagnetic capabilities (EMC) and training for human-machine interface.

APPENDIX 1

CASE STUDIES

Seven operational incidents were selected as Case Studies. They are summarised below, to illustrate the nature of the relationships that exist between NPP elements, including the human element, where stored-programme computers are employed. Lessons learned from these case studies are either included in the studies below, or have been highlighted in appropriate sections of the report.

Case Study 1 (USA)

Human-Machine Interface Error (LER 91-006-00*)*

On February 17, 1991, Unit 1 at the Limerick Generating Station experienced an actuation of the primary containment and reactor vessel isolation control system, an ESF resulting in the generation of a radiation isolation signal for the drywell and suppression pool purge supply and exhaust valves. This event was caused by selecting an "undefined" wide range accident monitor (WRAM) channel item number at the safety-related data access panel (RM-23) in the main control room.

An investigation revealed that personnel error caused this actuation. While interrogating the radiological meteorological monitoring system, the shift technical advisor (STA) and STA trainee selected a channel item number (i.e., 100) that is not listed in procedure RMMS-301. When the STAs selected this channel item number, the WRAM microprocessor repeatedly searched for non-existent data. The WRAM microprocessor was not able to complete the task of locating the requested data in the allotted time period, resulting in the error message. This error message caused the WRAM to initiate a system reset by momentarily disconnecting and connecting power. When the system reset, the relays in the WRAM lost power. One of these relays is associated with the actuation of the high radiation isolation signal for the primary containment and reactor vessel isolation control system. Therefore, when this relay momentarily lost power, it failed to its safe position (closed) and initiated the high radiation isolation signal for the drywell and suppression pool purge supply and exhaust valves.

Case Study 2 (Canada)

Software Coding Error Caused Pressure Boundary Damage (IRS No. 1118.00)

Background

Fuelling on the CANDU reactors can be carried out while the reactor is on line. A fuelling machine (FM) moves into place near a reactor. There is one fuelling bridge at each end of each reactor. The bridge picks up the FM, positions the FM at the reactor face, and the FM head locks onto a fuel channel. The fuel channel carries both the fuel, and pressurised heavy water (D2O). The D2O removes the heat from the

fuel and transfers it to the boilers. This system is called the primary heat transport system (HTS). A FM head must lock onto each end of the channel, one handled by each bridge. The FM heads then must be pressurised to the pressure of the HTS. End plugs are then removed and some new fuel is pushed in from one end, and spent fuel is pushed out of the other end. End plugs then are replaced.

The FM is computer controlled. There are three computer systems and three FMs. Each computer system consists of two or three computers, with a total of eight computers. In general, one computer system controls one FM. However, as each FM can be positioned at any reactor (with some limitations), it is clear that each computer system must have the capability to control any of the bridges.

Event description

This event occurred on 23 January 1990. A FM was clamped onto a channel of unit 4 and was in the process of being filled and vented but it was not pressurised. The bridge at the east end of unit 4 unexpectedly moved downwards about 40 cm which caused damage to the fuel-channel end fitting, onto which the FM was clamped. There was a loss of D2O, which is the primary HTS. The reactor was shut down and D2O had to be transferred from other units to maintain the HTS inventory of unit 4. A valve failure complicated the cool-down procedure. Shut-down was achieved safely and subsequently the spilt D2O was recovered.

Cause of the Event

The primary cause of the event was a software bug in the FM code. This bug had been introduced during a previous software upgrade. The bug in itself would not have caused a failure, and indeed had been in place for a considerable time, except that a number of other factors combined to cause the incident.

A previous error on one of the other FM computer systems (not the one being used for refuelling) had caused that computer to be 'primed' to call for the release of brakes on the unit 4 bridge. An operator carrying out an unrelated operation on this other computer system triggered the computer to 'remember' this previous event, and to call for a release of the brakes on the unit 4 bridge. One of the protective computers on this other system was out of commission, so it did not trap the call to release the bridge brakes on what should be a non-controlled system. Thus this other computer released the brakes on the bridge which was being used for refuelling.

Identified Deficiencies

The primary cause of the incident was a software bug in the FM code. In addition, the following deficiencies were also identified:

i. One of the computers was out of service. If it had been in service it would have prevented the movement of the bridge.

ii. The operator working on the other computer system, which released the brakes on unit 4 bridge, was unable to determine whether a warning lamp was on or off.

iii. The ability of any computer system to control any bridge should be safeguarded by mechanical interlocks, not just software interlocks.

iv. Once locked onto the reactor face, the bridge brake and motor controls should be electrically isolated to prevent bridge movement.

Corrective Action

As a result of this incident, the operating authority has implemented the following changes:

i. A complete inspection and repair has been carried out on the damaged reactor components.

ii. The software bug has been rectified.

iii. A hazards analysis of the FM software has been undertaken to identify other possible latent problems.

iv. Investigations were started to review the design philosophy of the FM protective system.

v. A quality control programme was put in place for all software changes.

Case Study 3 (Canada)

Pickering Emergency Response Projection (PERP) Code Discrepancy (IRS No. 1452)

Event description

The Pickering Emergency Response Projection (PERP) computer code is used for making projections of doses that would result from an airborne release of radioactive materials following a nuclear accident, for the area surrounding Pickering Nuclear Generating Station (NGS). Version 1.00 of the PERP code was issued in May 1993, and was the latest in a series of a new generation of emergency response codes written for the various NGSs.

Prior to using PERP, Pickering NGS had been using a code called ERP, issued in 1987. This code was used in conjunction with a manual calculation algorithm, based on the ERP results. The purpose of the Manual Calculation was to provide a preliminary assessment of dose rates for the first few hours following the initiation of venting, and before the ERP code had been put in operation. PERP was issued with the implicit understanding that it would supersede ERP, and that the Simplified Calculation module of PERP would replace the Manual Calculation.

In the course of preparing a drill, Pickering NGS staff found a large discrepancy between a dose rate calculated using version 1.00 PERP and a corresponding value obtained from the Manual Calculation. The PERP code was found to have the potential to overestimate releases and doses to the public by up to a factor of twenty when compared to the Manual Calculation, which was based on an early version of ERP.

Causes of the event

The investigation found that there were three sources for the discrepancy:

i. Differences in the way processes were modelled in ERP and PERP, reflecting a change in the preferred mode of operation of the filtered air discharge system (FADS) between the time the two codes were written. It is a valid change but it was not elaborated to the operational staff.

ii. Some data and parameter values used in PERP and ERP were different. Some of the changes were deliberate and reflected changes in assumptions made in the safety report. Other changes were unintentional, with some factors being counted twice.

iii. There was a programme coding error in the Source Term Adjustment (STA) module of PERP which resulted in some elements being missed in the dose rate calculation.

Identified deficiencies

The following deficiencies have been identified by the regulatory agency:

i. A lack of comprehensiveness in the verification methods used, which allowed an error in the STA routine to remain undetected.

ii. The absence of formal procedures for issue of new versions of the code, which led to a failure to supersede the outdated Manual Calculation method with the Simplified Calculation module of PERP.

iii. A lack of awareness of the modelling assumptions used in the two methods and the sensitivity of code predictions to these modelling assumptions, particularly in the first few hours after discharge begins.

iv. Lack of a clear policy to inform users of any known discrepancies prior to the issue of revised versions of the code, even if such discrepancies were known and judged to be minor.

Corrective actions

The following actions have been taken since the incident:

i. A revised version of PERP has been issued, which incorporates the latest data available and corrections for the subroutine in error. Revised versions of ERP currently in use at Bruce NGS (BERP) and at Darlington NGS (DERP) also have been issued.

ii. PERP, BERP, and DERP will comply with the RSOAD software QA programme.

iii. Actions have been initiated to remove the outdated Manual Calculation from Pickering NGS Operating Procedures.

iv. The code has been subjected to a thorough review as part of the investigation and the identified discrepancies have been fully accounted for.

v. In addition to the above detailed review, a further series of comparisons against the latest results from Safety Reports has been planned to ensure consistency. Such comparisons will be carried out every time a new Safety Report is issued.

vi. A policy will be adopted to keep users informed of code status in the event that a need for modifications is identified.

Lessons learned

i. The many problems encountered with the software code, the changes in the modelling methods, and the errors in the data and parameter values indicates a lack of strict software configuration and quality control.

ii. The code was installed at Pickering in May 1993 but, apparently, was not tested on site until March 1994. The users of new software should carry out their own quality checks on receipt of new software, and before it is put into service, otherwise defective software may be used in an emergency.

iii. A lack of communication exists between the authors of software and the users, with respect to the algorithms and assumptions made.

Case Study 4 (Canada)

Unit 2 Loss of Regulation (LOR) from Low Power (IRS No. 1360)

Event description

This event occurred on 15 November 1992. The reactor had been out of service for more than a year and staff were in the process of restarting the reactor. Criticality had been reached and reactor power was at -3 decades. Reactor power started to increase unexpectedly and the reactor regulating system (RRS) initiated a step-back on high log rate of power increase. It caused a step-back by partially inserting the mechanical control absorbers (MCAs). This reduced the rate of rise of power, and the RRS withdrew the MCAs. As soon as the MCAs were withdrawn, power again increased, causing another step-back, and partial MCA drop. As power stabilised, the RRS again withdrew the MCAs, and again the reactor power rose. This time power rose above the limit of the SDSs, and SDS1 tripped and shut down the reactor.

A technician had been authorised to work on one of the three ion chamber (IC) signals driving DCC-X and DCC-Y (Channel A). The ICs measure reactor power when the reactor is at low power levels. Although the Authorised Nuclear Operator (ANO) had authorised the work, the sensor had not been jumpered out at the time that the technician started to work. This reason was assumed to be the cause of the loss of regulation, so the channel was jumpered out and the reactor power again was increased. Once again a number of step-backs occurred, followed by an SDS trip on high power.

Cause of the event

Normally there are three IC signals available to the RRS. Rules for use of the three signals are:

i. With all three signals available and rational (within defined ranges), the RRS selects the middle value channel.

ii. With one channel below normal, the RRS selects the higher of the other two signals.

iii. If two signals are irrational, the RRS shuts down.

When the reactor is shut down for a long period, power will fall to very low levels, and the RRS could shut down completely, as two IC signals may fall below acceptable ranges. Thus a patch is put in the software to tell the RRS to bypass the rationality checks. This means that the RRS will always select the middle signal.

In this case, the reactor was restarted with the patch still in place. In addition, channel B IC had a faulty diode in its amplifier, which caused channel B to always read -4.1 decades. If the patch had not been in place, and with channel A out of service, the RRS would have used the higher IC reading, which would have been channel C, the only IC which was, in fact, working. Start up would have proceeded normally.

As the jumper had been left in place, it saw channel C reading high, channel A reading - 7.9 decades (after the technician started working on it), and it selected channel B as the middle reading channel. Channel B was, in fact stuck, at -4.1 decades, so the RRS kept removing negative reactivity in an attempt to increase

power to the required -3 decades. According to its sensor (IC channel B), power did not increase, so more and more negative reactivity was removed until the actual rate of increase in power caused a step-back.

Comments

For this event to occur, three things had to happen at the same time:

i. The technician took IC channel A out of service.

ii. IC channel B was defective.

iii. The software 'very low power' patch was left in place when it should have been removed.

In addition, the operating staff misdiagnosed the problem the first time, then tried a second restart with the same set of conditions in place.

Identified deficiencies

The utility and AECB identified the following deficiencies associated with this event:

i. Procedures applicable to patching the software did not detail when the patch should be removed.

ii. Risks associated with removing rationality checks had not been fully assessed.

iii. The operations' manual did not give clear instructions regarding the applicability of patches.

iv. The work on the ion chamber did not take into account the start up of the reactor.

v. The SDS response procedure was inadequate.

vi. The display system was deemed to be inadequate to identify the problem rapidly and prevent it.

vii. A faulty diode was not identified prior to start up.

viii. The staff failed to identify the cause of the first loss of regulation correctly.

Corrective actions

As a result of this incident, the operating authority has implemented the following:

i. The operations' manual has been improved to clarify actions in the event of a step-back.

ii. Procedures have been revised to give explicit instructions regarding software patches.

iii. The failed diode was replaced and the failed unit was analysed. No 'pattern' failure mode was found.

iv. This type of event has been included in operator training.

v. A permanent solution for the very low power patch is being investigated.

vi. Procedures are being updated to clarify further when and how maintenance can be performed on the ion chambers.

vii. Safety system tests are being designed for the regulating panel.

Lessons learned

The following lessons have been learned [AECB Accident Investigation Team, 1994], and should be applied to all nuclear installations:

i. The existing procedures for temporary patches were found to be inadequate.

ii. An assessment of the trip reset philosophy is needed.

iii. A potential problem exists in the step-back system, as it 'cycled' before the cause of the problem was found.

iv. Patching of the software is a risk-laden exercise, especially as the patch can be put in wrong and, as in this instance, the patch was not removed when it should have been. The software should be designed to handle these marginal conditions. For example, the removal of rationality checks could be programmed into the software, and when the operator calls for an increase in power above a pre-set limit, the very low power conditions could be removed automatically by the software. This situation would have eliminated the human error.

Case Study 5 (Canada)

A request for a Control Computer Printout Causes Reactor Shutdown

(IRS No. to be assigned)

Background

At Darlington nuclear power plant, a dual digital control computer (DCC) system is used on each reactor unit for control, alarm annunciation and data display. Both computers, DCC X and DCC Y, run at all times with the programme in both machines switched on. Each computer in this dual computer control system performs identical functions. Examples of these functions are reactor power control, overall unit control, steam generator level and pressure control, heat transport pressure and inventory control, and data logs.

Each computer is a modern high-speed machine with its own private main memory, solid-state disk memory, unit input output interface and peripheral equipment. The two computers communicate through a computer-to-computer data link. However, unit control by either computer is not dependent upon this data link. When DCC X is the controlling computer and the outputs from this computer are connected to the plant equipment, then DCC Y's outputs are disconnected. The system is organised so that maintenance on one computer can take place while the unit is being controlled by the other computer. A fault in any essential part of the master computer results in automatic transfer of control to the standby computer. If both computers fail, the unit is automatically shut down.

The reliability of this dual computer control system results from combining reliable solid-state hardware with a self-checking system. A number of critical hardware related tests are incorporated into a memory-resident hardware check task. Faults, either software or hardware, are detected by a combination of internal hardware and software self-checking plus external watchdog timers. Detection of a failure results in control being relinquished by the computer in which the failure occurs. A restart system, which automatically reloads the main memory from the disk memory and restarts the computer, is combined with the fault detection. Each computer is connected to an independent 120 V ac, class II bus.

Each unit system supports two high-speed printers. The printers and 14 cathode ray tube (CRT) display monitors are the principal means of communicating with the operator.

Description of the event

Unit 2 was operating at 99% full power. At 6:53 hr, with DCC X in control, DCC Y stalled without auto-restart. The unit authorised nuclear operator (ANO) contacted the computer maintenance (CM) group to investigate. The computer was left in the failed state to assist CM in investigating the cause of failure.

Four minutes later, DCC X stalled without auto-restart. As a result of the dual DCC failure, control absorbers dropped into the core and the liquid zones filled causing a reactor shutdown.

The ANO confirmed the power reduction and manually restarted DCC X and initiated further actions, as per procedures, to restore process system conditions to normal. DCC Y was restarted approximately two minutes later. The unit poisoned-out before the cause of failure could be determined.

With assistance from the technical support unit, an investigation was initiated into the cause of the dual DCC failure. Failure investigation found that an engineer, performing technical surveillance, requested certain data logged by DCC Y. Prior permission had been obtained from the ANO to retrieve the required logs. The request asked for information 48 hours earlier than the normal "last 12 hours" request. This request, although legitimate, has not been frequently used. The request caused DCC Y to stall.

As the engineer was in the control equipment room behind the main control room panel, he was unaware that DCC Y had stalled as a result of his request. He then made the same log request from DCC X about four minutes later. This caused DCC X to stall, resulting in a dual computer failure and unit shutdown.

Cause of Computer Failure

The computer stalls were called for by the self-check programme called hardware check (HCK). HCK normally looks for computer failures that could lead to problems with reactor control, however, in this case, it did not find actual control deficiencies. It called for a stall because of the inability of the hardware to successfully complete a specific HCK test. The test could not be successfully carried out because of an apparent time delay in retrieving the logged data. The event was recreated many times and, on some trials, the computer did indeed stall.

Mechanism of Failure

Both stalls were caused when the HCK programme received a 'data late' error return from the fixed head disk (FHD) while it was conducting its write check tests. The HCK programme checks the memory image of the reactor regulating system programme, the stepback monitoring programme and itself every two seconds against the equivalent images on the FHD. This is accomplished through a feature of the FHD controller which allows it to compare main memory with the disk using direct memory access (DMA). The controller returns a success if no differences (corruptions) are found. HCK will stall the DCC if anything other than a success is returned.

The FHD hardware is designed such that it must transfer data to or from main memory within a specific time. If the transfer is not completed in the allotted time the FHD controller will raise a 'data late' error.

The FHD software driver, which provides the interface between the hardware and applications programmes such as HCK, retries a failed transfer once before reporting the result back to the application programme. Therefore the DCC stalls were caused when two back to back write check attempts failed with a 'data late' return code.

The stalls were initially thought to be caused by the moving head disk (MHD) activity, generated by the log request, interfering with HCK's write check operations. Both the MHD and FHD are DMA devices. If they are transferring data to or from memory at the same time their transfers would be interleaved. This might have been enough to delay the FHD controller from getting hold of the bus in time to avoid a 'data late' error. The type of log request which caused the stalls initiates a higher level of MHD DMA activity than a normal log request. Subsequent testing in the lab and a more detailed review of the stall data showed this was not the case.

The stalls were caused when a tight loop in the logging software was executed as a result of the system engineer's log request. The tight loop was shown to delay the FHD's DMA activity long enough that a 'data late' error would occur. If the FHD transfer happened to be from the HCK write check test a stall might occur (about one stall per 10 log requests).

The logging subsystem maintains 48 hourly samples of data on the MHD. When a shift log is requested the data shown defaults to the last 12 hourly samples unless otherwise requested. If the user wants anything other than the default, the last hour and day to appear on the log must be entered. If none of the data is available on the MHD the request is not allowed. If some of the data is available it is output on the log in its respective columns; the remaining columns are initialised to indicate no data is available. The initialisation process involves clearing a block of 31000(8) words of main memory using a 'clear' instruction in a tight loop.

The 'clear' instruction belongs to a class of instructions which blocks DMA activity for two bus cycles. A review of the stall data and lab testing showed that a 'clear' loop in the range of 15000(8) words could stall a DCC by slowing down the DMA transfer rate of the FHD. Loops below this threshold tended to cause recoverable 'data late' errors (i.e. the second transfer attempt was successful).

Tight loop tests were performed using other instructions such as moving a zero into a memory location instead of clearing it. The move instructions does not block DMA for two bus cycles. The same size loop caused recoverable 'data late' errors at a rate of about one per five minutes (i.e. no DCC stalls). However this suggests that larger size loops could also stall the DCC or cause failures of FHD transfers. These tests indicate that the present FHD can transfer data faster than the DCC can accept or provide it when main memory is being accessed. This causes the FHD controller to experience 'data late' errors.

Human Factors

The system engineer who requested the logs which initiated the DCC stalls was not aware that the first DCC had stalled before requesting the same data from the other DCC. There are DCC status indicating lamps on the maintenance panel where the log requests were initiated. The lamps indicate which DCC is master, exercising control, stalled, has a flasher fault or has a temperature/cooling air flow problem. All the lamps are white. The stall, master and exercising control lamps are located near the bottom of the panel just above the DCC keyboard. The engineer did not notice that the lamps had changed state when the first DCC stalled. However the engineer said this would not have deterred the log request from the remaining DCC.

Actions taken by the Utility

- In the short term, this type of log request will no longer be allowed.
- Revise operating instructions to define what log options can be used and when.
- Consider revisions to operating instructions on a DCC stall to eliminate unnecessary requests on the remaining DCC. Consider bringing up the topic of DCC data requests at an information transfer session.
- Review alternatives to eliminate the use of a tight loop in the logging software.
- Determine if similar loops exist in other DCC applications and assess their significance.
- Assess the human factors issues related to the DCC status indications in the computer room and make recommendations.
- Conduct a detailed CPU, Unibus and memory access loading study of the DCC's. Attention should be given to peak loading periods and their effect on system performance. Provide recommendations on improving system performance based on findings from the study.
- Review the design of the FHD and provide alternatives to allow it to meet its performance requirements considering the above loading study and how DCCs operate. The effect of memory access loading on other devices needs to be reviewed.

Case Study 6 (USA) - October 22, 1996

NRC INFORMATION NOTICE 96-56: Problems Associated with Testing, Tuning, or Resetting of Digital Control Systems while at power

Description of Circumstances

Washington Nuclear Project 2 (WNP-2)

On July 20, 1996, the WNP-2 facility experienced a rapid change in power of 15 percent in a 40-second time frame. Specifically, power dropped from 68 to 53 percent and returned to 68 percent. The licensee determined that the power transient resulted from testing of the recently installed digital adjustable speed drive modification to the reactor recirculation pumps. The adjustable speed drive provides the capability to change the speed of the reactor recirculation pump motors and eliminates the need for recirculation flow control valves.

Before the event, the licensee was preparing to increase reactor recirculation flow from 51 to 53 percent. As part of the preparation, a non licensed General Electric (GE) test engineer typed computer instructions that would return the reactor recirculation flow to 51 percent if electrical harmonics were experienced in the adjustable speed drive system during the reactor recirculation flow increase. Once these instructions were typed, a licensed reactor operator would verify the entry and only had to strike the "ENTER" key on the computer keyboard to execute the instruction. It was intended that the licensed operator would only hit the ENTER key and execute the instruction if the system started to experience electrical harmonics as reactor recirculation flow was increased. If there were no electrical harmonics, the instruction would not be executed. In this instance, the GE engineer typed an incorrect value (transposed numbers) and then

mistakenly executed the instruction by striking the ENTER key. These actions caused reactor recirculation flow and reactor power to drop.

Immediately after entering the data, the GE engineer recognised the error and corrected the instruction, thereby increasing reactor power.

Dresden Unit 2

On May 31, 1996, while at approximately 45-percent power, Dresden Unit 2 experienced a loss of reactor feedwater control and a subsequent decrease in reactor vessel water level while performing an on-line configuration change to the recently installed Bailey Network 90 digital feedwater control system. Operators initiated a manual reactor scram as a result of the decrease in the reactor vessel water level.

Before the event, the licensee was performing start-up testing of the Bailey Network 90 feedwater control system modification. During the start-up testing, the test team determined that a minor software logic change was required to correct a problem associated with automatic transition from the 2B feedwater regulating valve to the 2A valve. An original equipment manufacturer representative indicated that the proposed software logic change could be completed with the control system on-line. The manufacturer representative indicated that the system would check the logic before going into the control mode and, as a result, there would be no impact on plant operation. The test team reviewed and approved the on-line logic change; however, the approval process was not documented per station procedure.

The new software logic configuration was inserted on the backup control module. Automatic diagnostic checks indicated a successful load into the control module. Upon placing the backup control module in the execute mode, the 2B feedwater regulating valve began to close, resulting in a sudden drop in feedwater flow and reactor vessel water level.

During a subsequent design review of the Bailey Network 90 feedwater control system, a logic execution sequence error was found in the original logic design of the Bailey Network 90 firmware. This error caused the 2B feedwater regulating valve to close when the backup control module attempted to take over process control from the primary module. It was determined that the execution sequence error would have resulted in the same process control failure any time the backup control module attempted to take control from the primary control module with the control system in the automatic mode. This event is discussed in NRC Inspection Report 50-237/96-06 dated August 22, 1996

Browns Ferry Unit 2

On May 10, 1996, Browns Ferry Unit 2 experienced an automatic reactor scram on low reactor water level from full power. The low water level resulted from an unexpected runback of two of the three reactor feedwater pumps, which occurred while software parameter changes were being made in the recently installed digital feedwater control system. Specifically, the flow biasing of the feedwater pumps was being adjusted and the control system speed demand limit was being increased while at power in an effort to fine tune the system and thereby enhance system performance. When the software parameter changes were made active (saved) in the control system, a reinitialization sequence occurred within the control software block, which drove the feed pump speed demand signal to zero for a few seconds. Plant personnel were unaware that entering these new software parameters would cause the feedwater control system to reinitialise.

The cause of the event was attributed to inadequate design of the control system software. The digital feedwater control system is a Foxboro I/A distributed control system. The system software contains 380

software blocks, that is, logic functions performed by the computer. A design weakness existed in the installed system in that making software parameter changes in certain software blocks would cause the control system to automatically reinitialise to zero output. During its investigation, the licensee confirmed that for 5 of the 380 software blocks, a parameter change would result in a control system reinitialization.

This characteristic of the software design was not known to the plant personnel. As part of its corrective actions, the licensee modified the five affected software blocks to eliminate the reinitialization problem. This event is discussed in NRC Inspection Report 50-260/96-05 dated June 19, 1996 (Accession No. 9607030386).

Comanche Peak Unit 2

On May 5, 1996, while in Mode 3, Comanche Peak Unit 2 experienced an auto-start of the motor-driven auxiliary feedwater pumps while personnel were resetting the central processing units in the digital main feedwater pump turbine control system. Before the event, the vendor representative for the newly installed main feedwater pump control system requested access to reset the central processing units following completion of system testing. The shift manager cautioned the vendor and non licensed utility instrumentation and controls personnel that two of the three processors were required to be in service to avoid a trip of the main feedwater pumps.

The instrumentation and controls personnel and the vendor representative planned to reset the three central processing units one at a time to avoid initiating a trip of the main feedwater pumps. The first two processors were rebooted. However, during the reset of the third processor, an inadvertent trip signal was generated for both main feedwater pumps. This signal caused an auto-start of the motor-driven auxiliary feedwater pumps (an engineered safety feature actuation). All four motor-driven auxiliary feedwater flow control valves shifted to auto and opened. Both motor-driven auxiliary feedwater pumps were operating and supplying the required flow to the steam generators before the event.

The licensee concluded that the personnel performing the rebooting task did not adequately verify that the second processor was properly restored and functional before rebooting the third processor. The main feedwater pump trip signal was generated because the system sensed that two of the three central processing units were not functional.

Discussion

In recent years, many licensees have chosen to replace outdated analogue control systems with digital upgrades. Digital system retrofits are intended to improve system performance, reliability, flexibility, and operator interface characteristics.

These systems also offer the capability to change software parameters, setpoints, or logic configurations or to reset processors while at power. However, as illustrated in the events previously described, resetting processors in digital control systems or performing on-line software manipulations as part of digital control system tuning or testing can result in unforeseen transients, reactor trips, and engineered safety feature actuations.

The events described herein highlight the importance of evaluating proposed changes and developing and implementing controls for performing any type of on-line manipulation of digital control systems to avoid reactor transients and plant trips. When it is deemed necessary to reset a processor or to perform on-line software changes, it is important to maintain control of these activities in order to minimise potential

errors, and to be aware of the potential effect on plant operation if errors occur while performing such activities.

Case Study 7 (Japan)

Reactor Manual Shutdown due to the Reactor Coolant Recirculation PUMP Trip at Kashiwazaki-Kariwa Unit 6

Abstract

On February 23, 1996, during test operation, the output of Kashiwazaki-Kariwa Unit 6 (l356 Hew, ABWR) dropped, when the pump (C), one of ten reactor coolant recirculation pumps (RIP) tripped. Consequently, plant operators switched the control circuit (C1) to the control circuit (C2) in the power supply system to the affected RIP in order to restart the shutdown RIP and restored the output of the unit.

Later, the substrate of the failed control circuit (C1) was replaced with a new one and when the control circuit was switched back from (C2) to (C1), the RIP © tripped again. The unit was manually shutdown for examination and inspection.

The cause for the first RIP trip was the malfunction of the memory element in the control substrate.

The cause for the second RIP trip was misinput of the control constant data. The following countermeasures were taken:

(1) Modification in the control circuit switching function.

(2) Modification of the control constant feeding method when replacing substrates.

Event Description

The output of Unit No.6 of Kashiwazaki-Kariwa Nuclear Power Station dropped to about 265 MWe during its test operation at an output of 279 MWe around 9:35 pm on February 22 when Pump (C), one of the ten reactor coolant recirculation pumps (Reactor internal Pump [RIP]), tripped.

Consequently, plant operators switched the control circuit (C1) to the control circuit (C2) in the power supply system (RIP Adjustable speed Drive [RIP-ASD]) to the affected RIP in order to restart the shutdown RIP and restored the output of the Plant.

Later, the substrate of the failed control circuit (C1) was replaced with a new one, and when the control circuit was switched back from (C2) to (C1) at 8:25 am on February 23, RIP © tripped again and the plant output dropped to about 265 MWe. It was decided then to examine and inspect the plant and reduction in the plants output was started at 8:35 am on February 23. The reactor was shutdown at 11:05 am of the same day.

Investigation of the Cause

An investigation was made in to the cause of the RIP © trip. No abnormal condition was found with the RIP itself through the examination of the situation that caused the alarm to annunciate and also the relevant parameters such as the vibration of the RIP. Nor was any abnormal condition found with the input

transformer of RIP-ASD or with the motor of the RIP. On the other hand, while no abnormal condition was found with the power supply circuit section through inspection of RIP-ASD, an abnormal condition was found with control circuit section. The control constant of the operating control circuit (C1) which was in operation was abnormal; voltage at the smoothing capacitor was higher than normal level.

Further more the potential cause of having had abnormal control constant was analysed and evaluated. As a result, it was concluded that the possibility of the memory element malfunctioning in the control substrate cannot be denied.

It was also confirmed that the control data of the old substrate was fed into the new substrate when the control circuit (C1) was replaced.

Cause of the Event

(a) The cause that led to the RIP trip

The malfunction of the memory element fed the abnormal control constant into the control circuit (C1) which was in use at that time, causing automatic switching to the back up control circuit (C2). This switching process over-charged the smoothing capacitor in the Power supply circuit section of RIP-ASD. As a result, it also shutdown the control circuit (C2), leading to the RIP trip. At the test reproducing the event, the over-current is believed to have been brought about by a shift in phase.

(b) The cause for the second RIP trip

It was believed that the control constant data fed into the replaced substrate from the old substrate in use when this abnormal condition took place caused the second RIP trip.

Countermeasures

(a) Modification in the control circuit switching function

In order to assure proper switching of the control circuit, an adequate time for discharge is provided to allow the voltage of the smoothing capacitor in the power supply circuit section to decrease to a sufficiently low level.

Also, since the shift in phase may result by providing time for discharge, the phase will be adjusted after the discharge.

(b) Modification of the control constant feeding method when replacing substrates.

In order to prevent abnormal data of replaced substrates from mingling test control constants adjusted during test operations are to be stored on floppy disk each time. The control constants will be fed into new substrates from the disk.

REFERENCES

1. Fride, B. et. al, "Safety Assessment of Computerised Instrumentation and Control for Nuclear Power Plants", IPSN, 1995.

2. EPRI, "Guidelines on Licensing Digital Upgrades", EPRI TR-102348, Project 3373-04, Interim Report, December, 1993.

3. "Standard for Software Engineering of Safety Critical Software", Ontario Hydro and AECL, CE-1001-STD Rev. 1, 1995.

4. Lee, Eric J., "Computer-Based Digital System Failures", Technical Review Report, AEOD/T94-03, USNRC, July 1994.

5. Arsenault, James E., Manship, Roger A., "Operating Experience With Computer-Based Systems in Canadian Nuclear Power Plants", a report for the Atomic Energy Control Board, Ottawa, Canada, July, 1996.

6 R.M. Consultants Ltd., “An Investigation into PLC Software Reliability”, A report prepared for the Health and Safety Executive, London, U.K., November 1995.

7. Korsah K., Tanaka T.J., Wilson T.L., “Environmental Testing of an Experimental Digital Safety Channel”, NUREG/CR-6406, ORNL/TM-13122.

8. Kim, Hong-Woo, "Computer Maintenance Experience of Wolsong-1", 2nd COG Computer Conference, October 1-3, 1995, Toronto, Canada.

9. Austin, L., Do,Q., and Rannem, S., "Experiences from a Major Control & Monitoring Computer Rehabilitation Project", 2nd COG CANDU Computer Conference, October 1-3, 1995, Toronto, Canada.

10. Meslin, Thierry, "Ten Years of Experience Feedback on Computerized Operating Aid Facilities in Electicite De France - The lessons that can be drawn", OECD/IAEA International Symposium on Nuclear Power Plant Instrumentation and Control, Tokyo, Japan, 18-22 May, 1992.

11. Arsenault, James E., Manship, Roger A., "Review of Bruce A Reactor Regulating System Software", AECB Project No. 2.260.1, INFO-0616, December, 1995.

12. Habib, Tariq et. al., "Process Control Computers which lasted 27 years-Lesson Learned", 2nd COG Computer Conference, October 1-3, 1995, Toronto, Canada.10.