RSP-0034


# REVIEW OF THE RELIABILITY OF BRUCE 'B' RRS DUAL COMPUTER SYSTEM

FINAL REPORT

by

James E. Arsenault
Roger A. Manship
David G. Levan

The Liard Group Inc.
284 Liard Street, Stittsville, Ontario

A report prepared for the

Atomic Energy Control Board
Ottawa, Canada

30-01

28 July 1995

# REVIEW OF THE RELIABILITY OF BRUCE 'B' RRS DUAL COMPUTER SYSTEM

An assessment prepared by The Liard Group Inc., under contract to the Atomic Energy Control Board (AECB).

## ABSTRACT

The review presents an analysis of the Bruce 'B' Reactor Regulating System (RRS) Digital Control Computer (DCC) system, based on system documentation, significant event reports (SERs), question sets, and a site visit. The intent is to evaluate the reliability of the of the RRS DCC and to identify the possible scenarios that could lead to a serious process failure. The evaluation is based on three relatively independent analyses, which are integrated and presented in the form of Conclusions and Recommendations.

## RESUMÉ

## DISCLAIMER

## PREFACE

This document has been prepared for the Atomic Energy Control Board (AECB) by The Liard Group Inc. (TLGI), in accordance with Articles of Agreement dated 9 January 1995, in respect of Project No. and Title 2.339.1 - "Review of the Reliability of the Bruce 'A' ('*B*' ) RRS Dual Computer System".

The intent of this project is to evaluate the reliability of the Reactor Regulating System (RRS) Digital Control Computer (DCC) system and to identify the possible scenarios that could lead to a serious process failure.

The evaluation presents an analysis of the Bruce 'B' DCC system, based on system documentation, significant event reports (SERs), question sets, and a site visit. The evaluation proceeded along three relatively independent analyses, i.e., Failure Mode and Effects Analysis (FMEAs), Reliability Modelling, and SER Database Analysis which were integrated and are presented in the form of Conclusions and Recommendations. Recommendations are made with respect to software, hardware, and general issues.

The 13 possible scenarios, developed for Bruce 'B', were correlated with the SER database from 22 reactor units at all sites with the result that no matches could be established clearly. However, this does not mean that the scenarios developed could not occur at any time in the future. The reliability of the Bruce 'B' RRS DCC is in general agreement with predicted values and the reliability of all units combined has decreased steadily over the last 10 years and is also in general agreement with predicted values.

TABLE OF CONTENTS

LIST OF FIGURES



LIST OF TABLES

# 1.0 INTRODUCTION

## 1.1 Background

The Reactor Regulating System (RRS) in CANDU reactors uses two Digital Control Computers (DCCs) to control reactor power. Two redundant, identical computers continually monitor reactor conditions and determine the required adjustment of neutron absorbers to keep reactor power at the desired setpoint. The computers check both themselves and each other. One computer is controlling the reactor while the other is on standby, ready to take over if a self-check or a cross-check indicates that the controlling computer has a fault. If a fault is detected, the controlling computer has stalled (that is, stopped processing) and transfers the control to the standby computer. In some cases both computers can stall, which should lead to a fail-safe action known as a step-back operation and a subsequent reduction of reactor power.

In the event that the step-back fails and a loss of regulation occurs, two separate shutdown systems exist which will act to stop the chain reaction safely. A review of Significant Event Reports (SERs) has revealed events involving single computer stalls and dual computer stalls, with some of each leading to loss of regulation.

## 1.2 Objectives

The intent of this project is to evaluate the reliability of the dual computer system of the Reactor Regulating System at Bruce 'B' and to identify the possible scenarios that could lead to a serious process failure.

## 1.3 Scope

The project includes a review of the architecture (both hardware and software) of the dual control computers at Bruce 'B'. It identifies areas which have led to, or could potentially lead to, a common cause failure of both computers. The review encompasses:

- Transfer Logic
- Reactivity Devices
- Communications
- Alarm Units
- Operator Interface
- Inputs and Outputs
- Power Supplies
- Cabling.

In the course of the study, potential areas of common cause failures of both computers were identified. Some of these are safety related (serious process failure) and some relate only to a loss of production (electrical energy). Those which relate to a loss of production have been included for completeness but have been identified as not safety related.

In addition, the project considered the following possible conditions with respect to the RRS DCCs:

a. Failure to detect and/or to activate the fail-safe mechanism. This failure implies that the control absorber rods do not drop when required.

b. Failure to activate within the specified time, hence resulting in a delayed release of the control absorber rods.

c. Activation of the fail-safe mechanism, followed by an inadvertent deactivation, such as the release of the control absorber rods and their subsequent recapture before full insertion.

d. A failure of a hardware output (digital or analog) to achieve its fail-safe state.

# 2.0 METHODOLOGY

## 2.1 Introduction

The methodology progressed though a process of RRS system analysis, leading to a set of conclusions and recommendations. The methodology is described below in terms of inputs, processing, and outputs.

## 2.2 Inputs

The first stage involved a review of the RRS design documentation provided by the AECB. It should be noted that the design documentation was generally of a top-level nature and in some cases documents were contradictory. In parallel with this documentation review, a preliminary review of RRS Significant Event Reports (SERs) was conducted, involving stalls from all sites. At this point, the first series of clarifying questions was formulated. This set of questions was discussed with the AECB Headquarters staff and was forwarded to the Bruce 'B' site officer. Subsequently, a visit to Bruce 'B' was arranged and the questions were resolved via discussions between the AECB and Ontario Hydro site staff. During this visit, a tour of the RRS facilities was conducted. Additional sets of questions were forwarded to the AECB, which were subsequently resolved via discussion and refinement with AECB and Ontario Hydro site staff.

## 2.3 Processing

The design documentation reviewed certain specified RRS DCC availability requirements, on a computer basis, and provided a good understanding of the RRS DCC design intent at the system level. Responses to sets of questions and the site visit served to fill in and clarify the documentation. From this knowledge base, the development of possible failure scenarios was completed, using a narrative style, pseudo Failure Mode and Effects Analysis (FMEA) technique. From the same knowledge base it was possible to derive estimates for mean time between failure (MTBF) and mean time to repair (MTTR), taking into account both hardware and software. Aspects of as-built DCC performance, with respect to single and dual stalls, were derived from an analysis of the SER databases and copies of actual SERs. As there were very few SERs relating to Bruce 'B', the analysis included all nuclear power generation sites, to see if there was any correlation between the FMEAs specific to Bruce 'B', the Bruce 'B' reliability modelling, and the general SER database. Essentially, the analysis progressed along three relatively independent lines, which then were integrated to satisfy the project objectives, i.e., FMEA, Reliability Modelling, and SER Database Analysis.

## 2.4 Outputs

Based on the material developed via analysis and integration, the main points were summarized in the form of conclusions and recommendations.

# 3.0 DETAILED ANALYSIS

## 3.1 General

The RRS in CANDU reactors uses two dual Digital Control Computers (DCCs) to control reactor power. A functional block diagram of the RRS Control System is given in Figure 1.

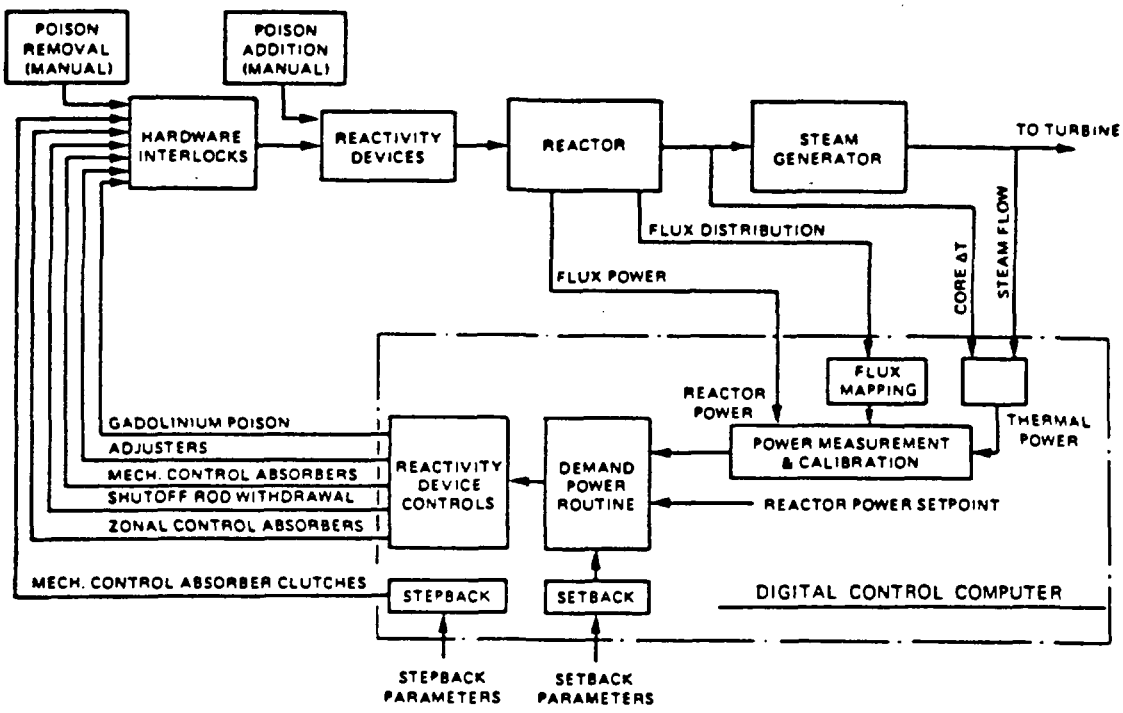


Figure 1. RRS Control System

Two redundant, identical computers continually monitor the reactor conditions and determine the required adjustment of neutron absorbers to keep the reactor at the required set point. The computers check both themselves and each other. One computer is controlling the reactor while the other is on stand-by, ready to take over if a self-check or a cross-check indicates that the controlling computer has stalled (that is, stopped processing) and transfer control to the stand-by computer.

In addition to controlling normal reactor power operation, the RRS DCC also incorporates features to ensure that the reactor enters a controlled safe state in the event that certain preset parameters are exceeded. These states are known as Setback, and Stepback. Reactor power set-backs are controlled reductions in power whereas step-backs can cause a reactor to shutdown rapidly to a preset power level via a control rod absorber drop.

### 3.1.1 Hardware description

The basic philosophy for the duplicated computer system is that all inputs required for essential functions are wired in parallel to each computer. Figure 2 illustrates the DCC system essential hardware.

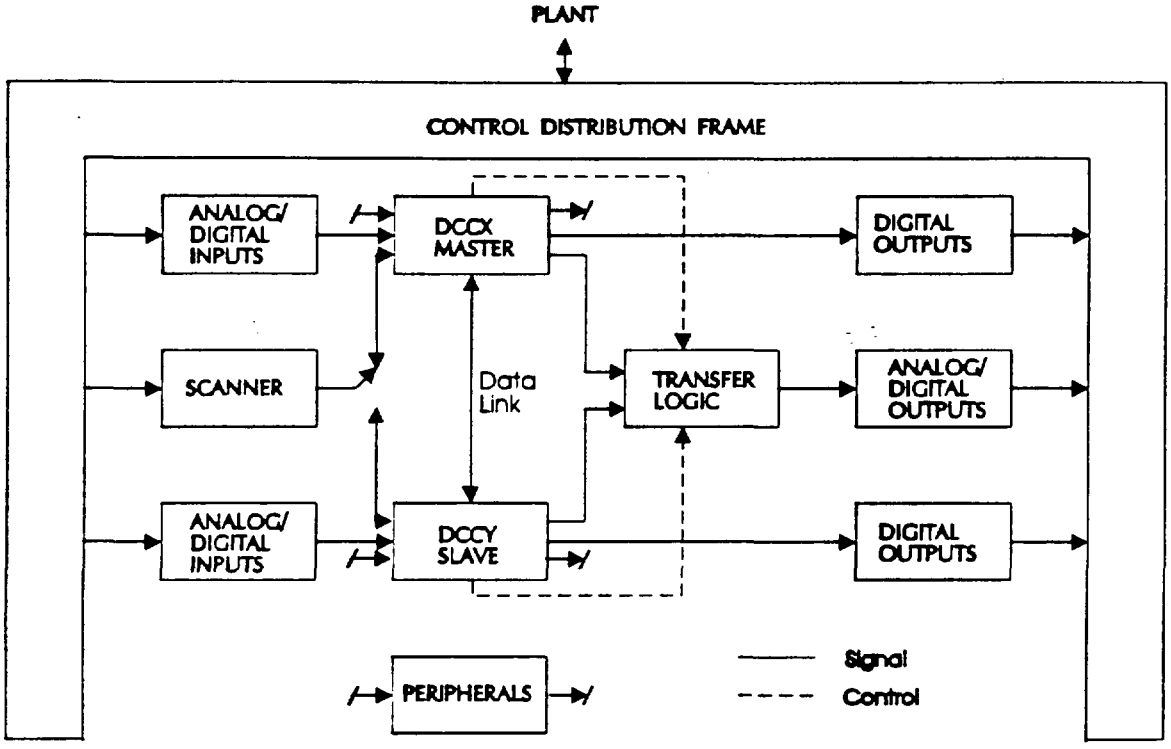


Figure 2. DCC System Hardware

All analog and digital inputs and critical digital outputs used for control are duplicated, and transfer of control via interlocking contacts is provided, to isolate these outputs from a failed computer. The majority of digital outputs are not interlocked but are just wired in parallel. In this case, only the controlling computer will activate its digital outputs. The input signals, both analog and digital, are derived from a common device and are wired in parallel to both computers. Duplicated or triplicated measurements of the same parameter also are wired in parallel to both computers. Functions not requiring the high availability are connected to only one computer. An example of this is the turbine run up (TRU) function. The control of mechanical control absorbers (MCAs) is implemented via a unique AND function which requires that both computers assert the need for a step back before it can be initiated. The wiring between the plant and the computer system is accomplished through a control distribution frame.

The two DCCX,Y computer systems are completely independent of each other, except for shared peripheral display controllers and computer-to-computer data link. A single digital scanner is provided for annunciation purposes only, which can be connected by a switch to either computer; DCCX normally is connected.

Each DCC employs two watchdog timers wired in series, such that the failure of either watchdog will cause transfer of control to the other computer. Failure can result from the absence of a programmed timeout or from a hardware fault.

The computer-human interface (CHI) is built around 10 independently operated, panel-mounted workstations, each consisting of a special-purpose keyboard and a full-graphics CRT terminal. All two-way communication between the plant operators or engineers and the DCC functions is effected through this facility. Most of the one-way communications (display and print only) also are initiated through this facility. The operator designates the Master-Slave relationship via a key switch mounted on the keyboard.

The reactivity devices controlled by the RRS DCCs are:

- 14 light water levels in the zones
- 24 adjuster rods
- 4 mechanical control absorbers
- Gadolinium addition to the moderator.

In addition, the RRS DCCs may withdraw the 30 shutoff rods subject to interlocks with the SDS.

### 3.1.2 Software description

The RRS DCC software consists of background executive loop and control programs driven by eight countdown registers (CDRs), the most relevant of which are shown in Figure 3.

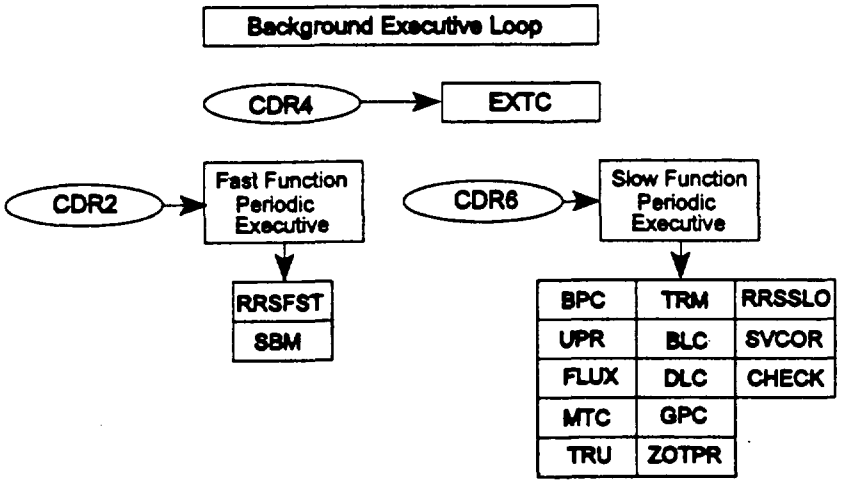


Figure 3. DCC System Software

For control purposes, each unit is divided into three main areas: Reactor, Boiler, and Turbine/Generator. There are three main interacting programs in the control loops, i.e., the

reactor regulating system (RRS), boiler pressure control (BPC), and unit power regulator (UPR) programs. Other programs, including step-back monitor (SBM), are involved in the control process. The program acronyms and formal names are listed below:

| | | | |
|---|---|---|---|
| BLC | Boiler Level Control | CHECK | Check Routine |
| DLC | De-aerator Level Control | EXTC | Executive Time Check |
| FLUX | Flux Mapping | GPC | General Purpose Control |
| MTC | Moderator Temperature Control | RRSFST | RRS Fast Loop |
| RRSSLO | RRS Slow Loop | SBM | Step-back Monitor |
| SVCOR | Save Core | TRU | Turbine Run-up |
| TRM | Turbine Monitor | ZOTPR | Zone Thermal Power |

The SBM monitors various unit parameters and if any one parameter exceeds a certain limit, a reactor step-back is initiated. Under normal conditions all programs are running in both X, Y computers. Control of the plant can be switched between DCCX,Y on a program-by-program basis. In 'normal' mode the RRS and BPC must be controlling from the same computer and have software checks to ensure that this happens upon control transfer. Each program has panel-mounted switches to give the operator control of the running programs. The control programs have the ability to turn themselves off individually when they are no longer capable of process control due to hardware or software failure. They have designated fail-safe tables for the executive to open/close their outputs upon failure.

Preset process conditions that are monitored by the SBM software are shown in Table 1, with the resulting percent of full power (FP) due to step back.

Table 1. Process Condition and Step-back Power Level

| Condition | Percent of full power |
|---|---|
| Reactor trip | 1 |
| Turbine trip or loss of line | 70 |
| Heat transport (HT) pump trip | 65 or 1 |
| HT pressure high | 1 |
| High zone flux | 1 |
| High rate log power | 1 |
| Low boiler level | 1 |

## 3.2 Type of System

The RRS is an important element in a multi-echelon approach to process protection, which is discussed more fully in Appendix D. The RRS is regarded as a safety-related system capable of causing a serious process failure in the absence of all special safety systems. The following definitions (draft), provided by the AECB, serve to place the foregoing sentence in perspective.

*safety related system* means a system, component, structure, or procedure (operator actions) and its support systems (including the special safety systems and their support systems) associated with initiation, detection, or mitigation of any failure sequence that may precipitate a serious process failure.

*serious process failure* means any failure of a safety related system that, in the absence of all special safety systems, could lead to systematic fuel failures or a significant release of radioactive substances from the nuclear power plant. Systematic fuel failures means that fuel with no prior defects fails as a consequence of the event. A significant release is one that would result in doses in excess of those of Table 4 for Class 1 events. Note: Table 4, Class 1 events are as per C-6, Rev. 0.

*special safety system* means one of the following systems: shutdown systems, emergency core cooling system (ECCS), and containment system.

The DCC system is, by design, dual redundant and is comprised of two nearly identical X, Y segments, so that in operation a unit outage is experienced only when both segments are not available. The design is best described as fault tolerant, in that segment failures may occur in the system but, as they are masked due to redundancy, no system failure occurs. In addition, it is important to note that failures are caused by faults. The degree of fault tolerance depends on familiar factors such as MTBF, MTTR, and the concept of fault coverage. When there is a segment fault that causes the master to stop processing (stall), the system will transfer control to the slave. In order to maintain a degree of precision in this document, the following definitions are formulated [Johnson, 1989].

*coverage* means the probability of fault detection, isolation, and fault recovery given that a fault exists.

*failure* means a deviation in the specified performance of an item.

*fault* means an imperfection that occurs in a hardware or software item.

*fault tolerance* means the ability to operate in the presence of failures.

A stall, i.e., a failure, usually will be caused by a hardware or software fault (human error is another possibility) in X, Y; the control will normally transfer from master to slave; and there will be no controlled process impact. However, from time to time, it can be expected that stalls will impact the controlled process in a range of effects up to, and including, a serious process failure. A stall may be single (one DCC) or dual (both DCCs).

*stall* means a cessation of processing.

*outage* means loss of unit power output to the grid.

## 3.3 RRS DCC System Availability Requirement

In document DD-29-66400-1, there is an expectation of Bruce 'B' DCC availability in excess of 99% per DCC, i.e., less than a downtime of 87.6 h/year per DCC. Also, it is indicated that prior experience with similar systems has shown forced unit outages of 8 h/year due to computer faults. Therefore, it is assumed that at Bruce 'B' the DCC computers should cause less than 8 h/year of unit outage. Assuming Bruce 'B' DCCs each have an availability of at least 99%, when used in a redundant pair configuration, the availability should be 99.99%, or a downtime of 0.876 h/year. Thus the forced unit outage due to a dual DDC failure can be expected to be less than 1.0 h/year.

## 3.4 RRS DCC System Analysis

The analyses, provided in subsections 3.4.1 to 3.4.3, have proceeded along three fairly independent lines, i.e., pseudo FMEA, availability modelling, and SER analysis. The results of the analyses are summarized at the end of each subsection and, finally, they are integrated in section 3.5.

### 3.4.1 Failure Mode and Effects Analysis

#### 3.4.1.1 General

The FMEA was carried out on the basis of the available RRS DCC software and hardware documentation listed in the Bibliography. It should be noted that some of these documents date back to 1982. Where clarification of these documents has been needed, Ontario Hydro and/or the AECB have provided additional information or clarifications. Section 3.5 discusses the correlation between the FMEAs and the SERs which were also studied to assist with scenario generation.

As a result of the analysis of the documentation, various failure scenarios have been postulated, which are documented in Appendix A using a pseudo FMEA technique to capture the relevant details systematically. The technique has followed the guidelines defined in MIL-STD-1629 [1980] but employs a narrative format rather than a tabular one, as this is more suitable to the objectives of this project.

It must be recognized that within the terms or time period of this contract, it has not been possible to validate these scenarios against the equipment, or against the detailed hardware and software documentation, schematics, and listings.

#### 3.4.1.2 FMEA classifications

To focus the analysis, the AECB has defined a classification scheme which relates directly to the Bruce 'B' RRS DCCs and is equivalent to the Severity Classification scheme of MIL-STD-781[1986]. These classifications are:

1. Failure of the system to detect and/or activate the fail-safe mechanism. This failure implies that the MCA rods do not drop when required.

2. Failure of the system to activate within the specified time, hence resulting in a delayed release of the MCA rods.

3. Activation of the fail-safe mechanism, followed by an inadvertent deactivation, such as the release of the MCA rods and their subsequent recapture before full insertion.

4. A failure of a hardware output (digital or analog) to achieve its fail-safe state.

Each scenario was reviewed and classified as appropriate. In the case where the scenario could not be placed in the classification scheme, it was designated as 'not applicable' (NA).

### 3.4.1.3 FMEA scenarios

Detailed FMEA scenario sheets are included in Appendix A. The following is a summary of those sheets and describes possible causes of a serious process failure, as defined in section 3.2.

RRS-1. The power supply which operates the clutch on the mechanical control absorber rods is not duplicated. A failure in this area would cause a rapid reduction in reactor power.

RRS-2. The two DCCs are not synchronized and enough time difference could exist to delay a power step back. This delay would result in the intervention of the Shut Down Systems (SDSs) to intervene and shut the reactor down.

RRS-3. A faulty data link between the two machines could write inadvertently into the memory of the destination DCC, thus corrupting the memory. Step-back could be prevented, thus requiring the SDS to intervene.

RRS-4. The priority interrupt system manages both the hardware and the initiation of software programs. A high level of traffic on higher priority devices could lock out lower level devices, such as the software control programs. The critical programs such as SBM would be delayed, and the SDS may operate before the RRS.

RRS-5. The software loading on the CPU may be higher than normally would be considered safe for a real-time system, which could result in some critical programs not running at the required time intervals. This would result in some critical functions, such as SBM, being late in responding to a plant problem.

RRS-6. Digital outputs, which are defined as critical to the correct operation of the plant, have been duplicated and wired in series. A single "stuck closed" failure cannot be detected, so a subsequent "stuck closed" failure would cause a critical situation to exist in the plant.

RRS-7. Although the relays on the circuit card assemblies are wetted mercury relays, the main relay banks consist of telephone-type relays which are exposed to the environment. The reliability of these relays is, therefore, in doubt.

RRS-8. Both of the DCCs are running identical software, so any residual software bugs in one machine will exist in the other. If one machine stalls on encountering a bug, there is a very high probability that the other machine also will stall.

RRS-9. The annunciation system relies on the background loop to display messages. Under heavy loading, the background loop may not run for up to 25 s. Annunciation

messages will be delayed and this may not allow sufficient time for the operators to rectify a problem.

RRS-10. The internal watchdog timer time-out has been set to a very long period, presumably because this is required by the high computer CPU loading. The long delay on the watchdog may mean that a DCC continues to operate the plant when it is not in a fully operational condition.

RRS-11. Because the SDS and the DCCs monitor different functions and use different sensors, it is possible that the SDS could detect a plant problem before the DCCs and, therefore, could shut down the reactor before the DCC has a chance to correct the situation.

RRS-12. The SBM program has design issues which mean that the MCA rods may be caught during a step back, even if a step back is still required. This effect will delay the reduction of reactor power and may cause the SDS to operate and to shut down the reactor fully.

RRS-13. The CHECK program may have insufficient coverage, which means that system faults may go undetected by CHECK which would prevent handing over control to the backup unit. A step-back condition could then be ignored, thus requiring the SDS to intervene.

#### 3.4.1.4 FMEA scenario summary

By reviewing the detailed results of the FMEA scenarios, developed in Appendix A, it is possible to group and prioritize them in terms of impact. The fundamental groupings are safety related, production related, and groupings where elements of both are involved to some degree. Table 2 presents an FMEA scenario summary, based on these considerations and the AECB classification scheme.

In constructing Table 2, the scenarios first were classified into groups and then were reviewed and prioritized in decreasing order for impact. For example, in the safety related group, DCC software loading was assessed as having the highest impact.

### 3.4.2 Reliability modelling

#### 3.4.2.1 General

Reliability analysis was performed to provide a theoretical base for comparison with results from the SER analysis and to support the project generally. For reliability analysis it is assumed that the RRS is comprised of dual redundant DCCX,Y computer segments and that they are symmetrical, i.e., identical. A complete reliability analysis of the RRS system is given in Appendix B and an outline of that analysis is given below.

#### 3.4.2.2 Segment MTBF

The segment MTBF refers to one half of the RRS DCC system. It should be noted that as the system is designed to be fault tolerant, most failures associated with one segment will not affect the safety of the system or production. The segment MTBF is derived from two sources, hardware and software.

Table 2. FMEA Scenario Summary

| No.[1] | FMEA Description | AECB Class |
|---|---|---|
| Safety Related[2]: | | |
| 5 | DCC software loading | 2 |
| 4 | DCC interrupt system | 2 |
| 12 | DCC SBM | 3 |
| 8 | DCC software bugs | 1 |
| 3 | DCC data link | 1 |
| 6 | DCC serial output contacts | 4 |
| 7 | Relay, control transfer frame | 4 |
| 2 | DCC synchronization | 2 |
| 10 | DCC watchdog timer | 2 |
| 13 | DCC CHECK program | 1 |
| Possible Safety Related: | | |
| 9 | DCC annunciation system (priority level) | NA |
| Not Safety Related; May Impact Production: | | |
| 1 | Power supply, clutch | NA |
| 11 | SDS/RRS interactions | NA |

Notes:
1. Scenario reference number.
2. Organized by group and decreasing impact .

The RRS electronics, except for peripheral equipment, such as CRT display monitors, keyboards, and printers, is mounted in a total of 14 steel cabinets and frames. For the generation of electronics of which the RRS is assumed to be typical, it can be expected that there will be an average of one failure per cabinet or frame/year [Assessment of..., 1994]. Therefore, about 14 failures/year can be expected to occur in the cabinet/frame electronics. With respect to peripherals, the keyboards generally have a very high MTBF and can be expected to contribute 1 failure/year. In addition, 1 failure/year can be expected to be contributed from the displays and printers. Note that most failures associated with displays and printers are of the wear-out variety and random failures are relatively infrequent, as equipment can be replaced "on condition" as deterioration is noted.

Overall, it can be expected that about 17 failures/year may occur in the RRS electronics. Assuming that the RRS X, Y electronics is symmetrical, about 8.5 failures/year can be expected for each of the RRS X, Y complement.

With respect to software, work described in Musa et al. [1990] and others demonstrates that it is possible to model software in useful ways that can allow reasonable predictions of software reliability to be made. Basically, a model is selected and is used to calculate the execution time failure rate, and then this rate is converted to calendar time, bearing in mind the particular approach taken to testing. For this study, the Basic Execution Time (BET) model has been applied, as it is most suitable for predictions. All of the the models depend on a variety of factors that have been identified as affecting software reliability, particularly the number of source lines of code (SLOC), processor speed, processor utilization (loading), and others.

To be developed effectively, the execution time/calendar time ratio requires a considerable amount of detailed information. This information is nearly impossible to estimate at this time, because the RRS software was developed (essentially) over 10 years ago. The inputs required for each of the three limiting test phases include knowledge with respect to the following resources: number of failure identification personnel, number of failure correction personnel, and CPU execution time. For each of these resources, the resource utilization must also be known. However, it is expected that calendar time would be of the order of 6 to 12 months.

To overcome the above difficulties, advantage can be taken of the fact that it can be assumed that the RRS software has been under continuous debugging for over 10 years. Also, it can be assumed that the software is operating in the computer execution time limitation phase, so that failures have a long failure interval. Experience shows that the the software can exhibit MTBFs in the thousands of hours, provided that the debugging effort is intensive. That this has certainly taken place is without question. Based on the above, it is expected that the RRS software should exhibit about 1 or 2 failures/segment/year.

For X, Y segments combined, it can be expected that hardware (17 failures) and software (4 failures) together will contribute about 21 failures, or an average of 10.5 failures/ segment/ year. However, practically none of these failures will propagate through to the RRS system level and result in unit outage, as the system is fault tolerant. An estimate of the system MTBF(s) can be derived on the basis of MTBF and MTTR of the segments. The segment MTBF is 8,760/10.5 = 834.2 h.

#### 3.4.2.3 Segment MTTR

As with segment MTBF, the segment MTTR must be based on both hardware and software but it can be approximated on the basis that:

- the segment is composed of replaceable modular electronics;
- modules are readily accessible;
- diagnostic aids, such as BITE, are thorough in isolating failed modules;
- equipment is maintained by experienced, well-trained personnel;
- hardware failures dominate; and
- software failures are circumvented by a manual reboot action when detected.

Consequently, it is estimated that most faults can be cleared and the system can be brought to normal operation in about one hour or less. This time estimate does not take into account administrative time, which includes obtaining spare modules, tools, etc., and may extend the effective MTTR to about four hours.

### 3.4.2.4 System reliability

Using the results from above, it can be shown that the MTBF of the RRS DCC system should be on the order of 20 years. This means that both of the DCCs will fail at the same time and cause a dual stall. This very large result is optimistic, because the calculation assumes a perfect switch-over mechanism and it does not account for uncovered faults. On the other hand, not all failures will result in a transfer of control, particularly in the case of peripherals, such as keyboards, displays, and printers. The system can be modelled more accurately with a Markov approach [Ibe et al., 1989] but the ready results given in Appendix B show that the MTBF(s) should certainly be on the order of several years. Indeed, the detailed analysis predicts an MTBF of about 20 years.

Assuming that there are a total of 22 licenced units operating with a unit MTBF of 20 years, it can be expected that there will be 22/20 = 1.1 unit outages/year caused by the RRS DCC system.

At Bruce 'B' there are four operational units and, assuming a single unit outage of 20 years, it can be expected that there will be a unit outage due to an RRS DCC failure about every five years at that site. The individual RRS DCC system associated with each unit can be expected to sustain about 21 failures/year, all of which should be masked due to the fault-tolerant design of the system and, therefore, they should appear to be transparent at the system level. However, these failures will lead to maintenance activities, such as circuit card replacement, manual computer restart, and so on. Table 3 summarizes the above discussion.

Table 3. RRS Reliability Prediction

| RRS failures/year[1] | Outages/year | |
|---|---|---|
| | Bruce 'B' [2] | All Sites[3] |
| 21.0 | 0.2 | 1.1 |

Notes:
1. Based on 1 unit. Masked due to fault tolerance.
2. Based on 4 units. Alternatively, 1 outage in 5 years.
3. Based on 22 units.

### 3.4.3 Significant event reports

### 3.4.3.1 General

SERs are required to be raised by licensees and to be submitted to the AECB in a timely fashion for review. The AECB, in turn, abstracts SERs into a database, which can be used to examine trends and to identify areas for further research and investigation. To support scenario generation and reliability analysis, a SER analysis was conducted at a very high level. Only a sample of SERs were reviewed in any detail, as the associated documentation was found too extensive.

### 3.4.3.2 Raw data

Initially, the AECB produced two SER listings covering the RRS at all nuclear generating sites, categorized as either single or dual stalls, essentially all of which involved a process impact up to, and including, a serious process failure. The listings covered the period from 1975 to 1994. Only two SERs were listed in 1975 and there was a data gap between 1975 and 1982. The data was found to be continuous from 1982 to 1994. Consequently, the two SERs entries from 1975 were deleted from analysis, on the basis of the small sample number, discontinuity, and absence of comparable older data.

The AECB provided the actual SERs for all nuclear generating sites for the last five years for more extensive review.

### 3.4.3.3 Classification

Each single and dual stall was classified, in terms of fault types. The data was then placed in a database for analysis purposes, the details of which appear in Appendix C. The 14 fault types and their percentages in decreasing order are given in Table 4.

Table 4. SER Fault Classification and Percentage

| Order | Fault Type | Percentage |
|---|---|---|
| 1 | Not specified[1] | 23.70 |
| 2 | Operator or process error | 9.83 |
| 2 | I/O sensor system | 9.83 |
| 2 | Peripheral | 9.83 |
| 3 | Other plant | 8.67 |
| 4 | Software | 7.51 |
| 4 | Other hardware | 7.51 |
| 5 | Fuse | 4.62 |
| 5 | Power supply unit (PSU) failure | 4.62 |
| 6 | Sensor failure | 4.05 |
| 7 | Memory parity | 3.47 |
| 8 | Memory other | 2.89 |
| 9 | Bad solder joint | 1.73 |
| 9 | Loose connection | 1.73 |

Notes:
1. The root cause of the failure could not be determined from the data provided by the AECB.

### 3.4.3.4 Analysis

The database contains 141 SER records from all locations. They were sorted twice: by year and by site (Appendix C, Tables C-1 and C-2, respectively).

From the sort of the database by year, it was found that the years with most and least stalls are 1983 (28 stalls) and 1994 (1 stall), respectively, with other years falling within this range. The largest fault type, at 23.7%, was 'Not Specified', which indicates that although stalls are recorded, the root cause was not clearly established at the time the SER was filed with the AECB. Thus it is possible that a more thorough review of the SERs would result in reassignment and a reduction in the 'Not Specified' category however experience shows that often up to one third of computer system faults can remain as "no fault found".

It is noted that all stalls occurring at Bruce 'B' were classified in a category other than 'Not Specified' indicating that that the root cause of the stall was determined in the course of SER analysis.

To illustrate the change of stall rate with time, Figure 4 gives a bar graph and three-year moving average of the number of stalls by year. It shows that the number of stalls has decreased steadily with time. It should also be noted that the large number of stalls in the earlier years would be expected as more units are brought on line, and the systems are debugged. As the systems become more mature in later years, a significant reduction in stalls can be expected, and should approach a steady state level.

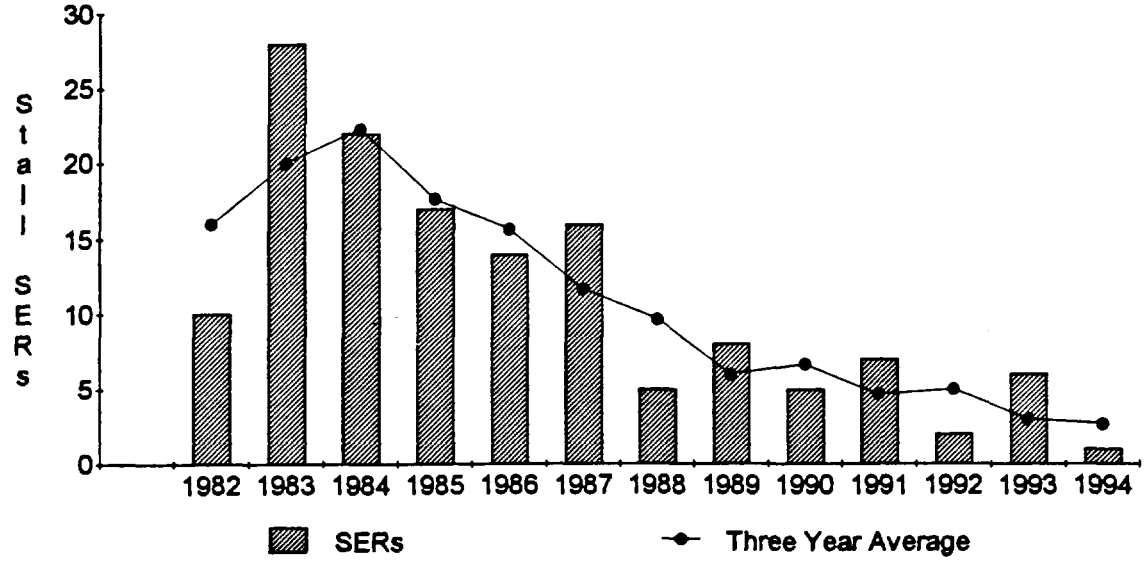


Figure 4. SER Stalls by Year

From the sort of the database by location, there was a total of six stalls between 1986 and 1994 at Bruce 'B', for an average of (6/8 =) 0.75 stalls per year. Four of these stalls occurred in 1986 and there was one stall in each of 1990 and 1991. If the 1986 data is removed, the stall rate is (2/7 =) 0.28 stalls per year, or one stall every 3.5 years. All of the stalls were of the single type.

## 3.5 System Analysis Integration

### 3.5.1 General

The DCC systems were studied in three ways: first, postulating failure modes and the possible effects on the operation of the plant, second, analyzing the significant event reports which have been provided, and third, a theoretical analysis of the reliability of the installed hardware and software. The following subsection seeks to correlate the data obtained from these three studies.

### 3.5.2 Integration analysis

The FMEA analysis postulated a number of scenarios.

There are four FMEAs which relate to the hardware: RRS-1, -3, -6, and -7. RRS-1 is the most significant, as it identifies an area of the hardware which is not redundant and where a single failure would shut down the reactor. This would be a fail-safe shut down but production would be lost.

The other hardware FMEAs postulate failure modes which have not, apparently, been observed by Ontario Hydro, or which are considered very rare events. However, as the equipment ages, more failures due to wear-out can be expected in the absence of a life extension program. It should be noted that failures in the relay logic would not, necessarily, affect critical plant areas and, therefore, normally will be covered by routine maintenance and an SER would not have to be raised.

The remaining FMEAs all relate to the software. There is no proof from the SERs that any of the postulated scenarios has occurred. However, there is no identified cause for 25.9% of the failures listed in the SERs (Table C.1 in Appendix C). In the event of a failure of the type defined in the FMEAs, it would be almost impossible to determine the exact cause of the failure after the event. Most of the FMEAs postulate a failure mode in which the RRS software is slow to operate and the SDS shuts the system down before the RRS can operate. Under these circumstances, there would be no permanent 'marker' in the software to show that anything out of the ordinary occurred. There is a possibility that the unexplained failures listed in the SERs were caused by latent software defects, of the type postulated in the FMEAs.

It should also be noted, that about one third of all software problems in any software system cannot be readily duplicated, traced, or adequately explained except through extraordinary effort. Thus, in this respect, the RRS DCCs are performing in line with industry norms.

The software reliability analysis predicts 1.15 dual computer stalls (outages)/year across all sites. The SERs indicate that, based on inputs from 22 reactors over 13 years, there have been 31 dual computer stalls, or an average rate of 2.4/year, which correlates reasonably well with the predicted rate.

A three-year moving average analysis of combined dual and single SERs showed that the number of stalls is decreasing, apparently exponentially, and may be approaching a steady state value. The three-year moving averages calculated for 1994 are 3.0 for combined dual and single stalls and 1.25 for dual stalls. The latter result is very close to the predicted value of 1.1. For all of 1994, only one stall was reported and it was of the single type. In general, the hardware and software comprising the RRS currently is meeting predicted reliability figures.

# 4.0 CONCLUSIONS

The review of the Bruce 'B' RRS dual computer system in the previous section leads to a number of conclusions. The conclusions are global in nature but are somewhat limited in detail, because of the effort applied being compatible with the scope and funding of this project. However, the conclusions are considered to be accurate and relevant in the context of the review.

## 4.1 General

### 4.1.1 Documentation currency

The documentation of the RRS DCC system reviewed does not represent the system as it now exists. This situation affects, and may limit, the generation of accurate failure scenarios, through possibly inaccurate understanding of the system's operation. For example, the hardware documentation makes no reference to certain items, such as the solid state, MegaRam store that replaces the fixed-head disk, or the floppy disk drive that replaces the paper tape reader/printer. A similar situation probably exists for the software documentation.

### 4.1.2 Limited analysis

The analysis accomplished is necessarily limited and is subject to improvement in all areas developed, because of the top-level approach employed. Much more detail would be required to assess the Bruce 'B' RRS DDC system further. This limitation applies to all three of the analytical threads pursued in the project (FMEA, Reliability analysis, SER analysis) and can result in imprecise system understanding (see 4.1.1), loose system boundary definition, and incomplete SER analysis.

## 4.2 Scenarios

### 4.2.1 Low correlation with SERs

The 13 scenarios postulated, based on an understanding of Bruce 'B' system operation, did not correlate well with the evidence derived from the SERs from all sites for known failures. However, this does not mean that any of the scenarios cannot occur at any time in the future. In addition, the lack of correlation may be an indication that the scenarios encompass at least some, or possibly most, of the underlying causes of the observed stalls in the cause not specified category (25.9%).

### 4.2.2 High processor loading

A common theme in many of the scenarios is related to processor loading. The CPU is, possibly, running at close to overload. In this particular case, i.e., for the Varian V-72, the relationship between processor loading and response times was not established.

## 4.3 SERs

### 4.3.1 Known causes

The SER analysis identified the causes of all failures for all stalls for Bruce 'B', as indicated in Appendix C, Table C.2. All of the stalls were of the single type.

For all sites the leading sources of known failures were: Operator or process failure (9.8%), I/O sensor system (9.8%) and Peripheral (9.8%).

### 4.3.2 Unspecified causes

Based on an analysis of the stall-related SERs from all sites, it was not possible, at this level of analysis, to establish a failure cause for 23.7% of the stalls recorded (this is not considered unusual compared to systems of a similar type). In addition, this is the largest failure category identified, which is usually an indication of hidden faults, for example, an intermittent solder joint or a software bug that recurs only infrequently. The amount of effort involved to cure such faults is, in some cases, very large and costly.

## 4.4 Reliability

### 4.4.1 Theory and measurement

At Bruce 'B', the reliability analysis prediction indicates that there should be about one outage every five years due to an RRS DCC dual stall, compared with an actual figure of no dual stalls logged in the SER analysis database. For all units, the expected outage is predicted to be 1.1 outages/year and for all of 1994 there was one stall (single) recorded. Thus, currently the RRS DCC appears to be causing events at about the expected rate.

### 4.4.2 Steady improvement

The reliability of the RRS DCC, based on the number of stall-related SERs generated annually from all sites, has decreased steadily since 1983. The shape of the three-year sliding average curve appears to be decreasing exponentially and may have reached a steady state value in the 1994 time-frame, i.e., about one stall per year. About 10 years has been required for the RRS outage value to agree, approximately, with predicted values.

# 5.0 RECOMMENDATIONS

The following recommendations are based upon the work carried out for this report, including:

- review of documentation;
- discussions held with the staff at Bruce 'B' generating station;
- failure mode and effects analysis;
- reliability analysis; and
- review of significant event reports.

It should be emphasized that the Bruce 'B' DCCs have proven to be very reliable to date but the DCCs at some other Ontario Hydro sites appear to be less reliable. In the absence of a life extension program the reliability at Bruce 'B' can be expected to deteriorate as the equipment ages.

## 5.1 General

### 5.1.1 Loading of the DCCs

A recurring issue in this report, and the underlying concern in most of the FMEAs, is that the computer response time may be too slow under high load conditions. The loading on the DCCs is believed to be about 85%. This loading needs to be verified and, if it is found to be high, steps should be taken to reduce the loading. Experience dictates that a loading of 50%-60% under average conditions is the maximum that should be tolerated on a real-time system. Once the loading has been reduced, the values used in the watchdog timer should be fine-tuned to provide better watchdog coverage.

### 5.1.2 RRS and SDS

An analysis should be carried out to determine the protection offered by the RRS and SDS, to ensure that the RRS is, in fact, detecting all possible error conditions before the SDS intervenes to shut down the systems.

### 5.1.3 System documentation

The documentation provided and referenced in this report was found to be inaccurate in some instances. Design documentation is critical to the maintenance of a large system and must be maintained at an accurate and current revision level.

### 5.1.4 SER procedures

The SERs are a valuable source of data but in the listings, in most cases, they do not provide a clear indication of root cause. In Addition, resulting actions do not seem to be cross-referenced between the SER and any resulting engineering change orders. The SER system should be operated as a closed loop system.

## 5.2 Software

### 5.2.1 SBM program

The SBM routine (according to the data provided) can inadvertently catch the MCA rods and, thus, delay a step back. The code should be checked to confirm this, and if so, it should be updated to remove the problem.

### 5.2.2 CHECK program

The CHECK routine is critical to the good health of the dual computer system. There is some concern that it may be deficient in some areas, which if found to be true, would require the CHECK program to be upgraded. A full analysis of the program is recommended.

### 5.2.3 Software patching

Software patching of an on-line system is a potentially hazardous and unreliable procedure. In general, the use of this technique in the profession has been eliminated over the last decade. All software modifications should be fully documented, reassembled, and retested off-line before being implemented on an active system. If patching is regarded as essential then a procedure should be developed for the purpose of controlling this activity.

### 5.2.4 Language

These DCC systems were written in Assembler code, which is very prone to errors. Any new DCC system software should be written in a language which is recognized as being suitable for safety critical applications, with a controlled and verifiable high-level language.

## 5.3 Hardware

### 5.3.1 MCA clutch power supply

The MCA clutch power supply is not duplicated and, therefore, is a single point of failure which can shut down the whole reactor system. Duplication of this element would greatly improve the inherent reliability of the system.

### 5.3.2 Duplicated digital outputs

The digital outputs, which are duplicated and wired in series for safety, are not tested on a regular basis to ensure that both contacts are still functional. To test these critical contacts, a simple test could be carried out during plant shutdown .

GLOSSARY

| | |
|---|---|
| AECB | Atomic Energy Control Board |
| AECL | Atomic Energy of Canada Ltd. |
| BEL | background executive loop |
| BET | basic execution time |
| BIC | buffer interface controller |
| BIOC | buffer input/output controller |
| BITE | built-in-test equipment |
| BLC | boiler level control |
| BPC | boiler pressure control |
| BPCS | basic process control system |
| CASE | computer-aided system engineering |
| CCFA | common cause failure analysis |
| CDR | count down register |
| CHECK | check program |
| CHI | computer-human interface |
| COTS | commercial off-the-shelf |
| CPU | central processing unit |
| CRT | cathode ray tube |
| DCC | digital control computer |
| DLC | de-aerator level control |
| DMA | direct memory access |
| ECCS | emergency core cooling system |
| EXTC | executive time check |
| FDDI | fibre distributed data interface |
| FHD | fixed head disc |
| FLUX | flux mapping program |
| FMEA | Failure Mode and Effects Analysis |
| FP | full power |
| GPC | general purpose control |
| HT | heat transport |
| HW | hardware |
| I/O | input/output |
| IEEE | Institute of Electrical and Electronic Engineers |
| IPL | independent protection layer |
| ISR | interrupt service routine |
| LAN | local area network |
| MAD | moving arm disk |
| MCA | mechanical control absorbers |
| MTBF | mean time between failure |
| MTC | moderator temperature control |
| MTTR | mean time to repair |
| PIM | priority interrupt module |
| PS | power supply |
| PSU | power supply unit |
| PTR | paper tape reader |
| RAID | redundant arrays of independent disks |
| RRS | reactor regulating system |

| | |
|---|---|
| RRSFST | RRS fast |
| RRSSLO | RRS slow |
| SBM | step-back monitor |
| SDS | shut down system |
| SER | significant event reports |
| SIL | safety integrity level |
| SIS | safety interlock system |
| SLOC | source lines of code |
| SMP | symmetrical multiprocessing |
| SPF | single point of failure |
| SVCOR | save core program |
| SW | software |
| TRM | turbine monitor |
| TRU | turbine run up |
| UPR | unit power regulator |
| WDT | watchdog timer |
| ZOTPR | zone thermal power |

## REFERENCES


-----. 1994. Assessment of User Experience with General Automation (GA) Computer Hardware, AECB, Ottawa, ON, 24 p. plus appendices.

-----. 1994. Evaluating software for safety systems in nuclear power plants. In: Nuclear Power Plants, Proc. of Ninth Annual Conf. on Computer Assurance: COMPASS '94, Lawrence Livermore National Laboratory, U.S. Nuclear Regulatory Commission, IEEE,NY.

----. 1994. Functional Safety: Safety-related Systems, Part 3: Software Requirements (Draft), TC65A, International Electrotechnical Commission, Geneva, Switzerland.

-----. 1986. MIL-STD-781D, Reliability Testing for Engineering Development, Qualification, and Production, U.S. Department of Defense, Washington, DC, 39 p.

-----. 1980. MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, U.S. Department of Defense, Washington, DC, 40 p. plus appendices.

----. 1988. MIL-STD-2167, Defense Systems Software Development, U.S. Department of Defense, Washington, DC.

----. 1993. Service Life Extension Assessment (Draft), Reliability Analysis Center, Rome, NY.

---. Consultative document C-6, Requirements for the Safety Analysis of CANDU Nuclear Power Plants, AECB, Ottawa, ON, Rev: 0.

Ibe O.C., R.C. Howe, and K.S. Trivedi. 1989. Approximate availability analysis of VAX Cluster Systems. IEEE Transactions on Reliability, Vol. 38, No.1, April 1989, 146-152.

Johnson, B.W. 1989. Design and Analysis of Fault-Tolerant Digital Systems. Addison-Wesley, Reading, MA, 584 p.

Musa J.D., A. Iannino, and K. Okumoto. 1990. Software Reliability, Measurement, Prediction, Application; Professional Edition, McGraw Hill Publishing Co., New York, NY, 291 p.

Rau, J.G. 1970. Optimization and Probability in Systems Engineering, Van Nostrand Reinhold, New York, NY, 402 p.

BIBLIOGRAPHY


-----. AECB Significant Event Reports (SERs): A summary of single DCC stalls. No report no., Sept. 08, 1994, 23 p.

-----. AECB Significant Event Reports (SERs): A summary of dual DCC stalls. No report no., Sept. 08, 1994, 8 p.

-----. AECB Significant Event Reports (SERs): Copies of stall related SERs for years 1989 through 1994, 62 p.

-----. Bruce 'B' Generating Station, Safety Report, Vol. 1, Section 6.0, Instrumentation and Control. Ontario Hydro, AECB ISN 25945, 1988, 18 p.

-----. Bruce 'B' Generating Station, Safety Report, Vol. 2, Section 3.3, Control Failures. Ontario Hydro, AECB ISN 25947, 1988?, 126 p.

Buijs, W.J. Digital control computer software, Part 5: control programs, Bruce Generating Station 'B'. AECL Engineering Co., DM-29-66700.5, AECB ISN 8860, 1982, Rev. 02 1989, 348 p.

Jelveh, M.R. Digital control computer software, Part 3: CRT display system, Bruce Nuclear Generating Station 'B'. AECL Engineering Co., DM-29-66700.3, AECB ISN 9675, 1982, Rev. 02 1988, 472 p.

Jelveh, M.R. Digital control computer software, Part 4: CRT man-machine interface, Bruce Nuclear Generating Station 'B'. AECL Engineering Co., DM-29-66700-004, AECB ISN 9676, 1982, Rev. 02 1989, 385 p.

Saari, M.E. Bruce Generating Station 'B', digital control computer software, computer annunciation system. AECL Engineering Co., DM-29-66700.1, AECB ISN 9673, 1982, Rev. 02 1986, 155 p.

Saari, M.E. Digital control computer software, Part 2: data acquisition. AECL Engineering Co., DM-29-66700.2, AECB ISN 9674, 1982, Rev. 02 1984, 83 p.

Schafer, S. Off-line disc operating system, Bruce 'B' Generating Station. AECL Engineering Co., DM-29-66600, AECB ISN 9664, 1981, Rev. 01 1982, 100 p.

-----. Unknown Publication. Annex 1, Instrumentation and control concepts for CANDU reactors: A Canadian example. No report nos., no date (early 1980s?), p. 155-207.

Walsh, R.D. Computer system executive and common routines. AECL Engineering Co., DM-29-66500, AECB ISN 9663, 1981, Rev. 02 1989, 188 p.

Wang, B.C. Bruce Generating Station 'B', long term historical data storage and retrieval system. AECL Engineering Co., DM-29-66600-2, AECB ISN 13766, 1984, 95 p.

Whan Tong, H. Computer hardware, Bruce 'B' Generating Station. AECL Engineering Co., DM-29-66400-1, AECB ISN 5061, 1989, 125 p.

Whan Tong, H. Digital control computer system, Bruce 'B' Generating Station. AECL Power Projects, DD-29-66400-1, AECB ISN 1202, 1979, 23 p.

APPENDIX A

# DETAILED FAILURE MODE AND EFFECTS ANALYSES SCENARIOS

## A.1 FMEAs

The following pages present the pseudo Failure Mode and Effects Analyses (FMEAs) scenarios carried out for the RRS DCCs. For ease of reference the AECB classification codes are provided below.

## A.2 AECB Classifications

1. Failure of the system to detect and/or activate the fail-safe mechanism. This failure implies that the MCA rods do not drop when required.

2. Failure of the system to activate within the specified time, hence resulting in a delayed release of the MCA rods.

3. Activation of the fail-safe mechanism, followed by an inadvertent deactivation, such as the release of the MCA rods and their subsequent recapture before full insertion.

4. A failure of a hardware output (digital or analog) to achieve its fail-safe state.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-1

NOMENCLATURE: Power Supply, Clutch

FUNCTION: The power supply (PS) provides current to the clutch holding relays (four) which, in conjunction with the electromechanical clutches, keep the mechanical control absorbers (MCAs) suspended over the reactor core.

FAILURE MODES AND CAUSES: Loss of PS current output to clutch relays caused by random component failure.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: All four clutch relays open and the four associated MCAs drop fully into the reactor core.

B. NEXT HIGHER LEVEL: The reactor power output drops as if a full step back had occurred.

C. END EFFECTS: Unit power output unavailable to grid.

FAILURE DETECTION METHOD: RRS reflects complete unit status to the Operator.

COMPENSATING PROVISIONS: Full rod drop produces a reactor safe condition.

AECB CLASSIFICATION: N/A, production issue only.

REMARKS: This failure mode identifies a single point of failure (SPF). In addition, if the PS is associated with only one mains power bus then this would represent another SPF. Typical PSs may be expected to exhibit MTBFs of 100,000 h or more in this type of environment, which can be described as Ground Benign. Note that, since there are four units at Bruce 'B', the combined MTBF is 25,000 h.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-2

NOMENCLATURE: Digital Control Computer Synchronization

FUNCTION: Two embedded DCCs (X, Y) are used in a dual redundant, master-slave arrangement to implement high availability process control associated with the RRS. In general, the machines run asynchronously, except that the machine clocks are synchrononized each hour by the plant clock. From that point the machines operate asynchronously and an alarm is raised when the machine clocks differ by 1 min. The RRSFST program, which encompasses the step-back function, runs every 0.5 s and, therefore, the worst-case time difference between the two machines could be as high as 0.5 s. The step-back function is implemented via AND logic, which requires that both DCCs assert that a step-back is to be initiated.

FAILURE MODES AND CAUSES: Delay in execution of the step-back function group up to 0.5 s, due to asynchronous operation of the DCCs.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: DCCs operate asynchronously and, therefore, may send time-delayed signals to the decision logic, both of which are necessary to initiate an MCA drop.

B. NEXT HIGHER LEVEL: The decision logic does not initiate an MCA drop until both DCC signals are presented to the AND logic, which could be delayed for up to 0.5 s. Consequently, the MCA drop may be delayed and, in the interim, the SDS may trip.

C. END EFFECTS: Unit power output unavailable to grid.

FAILURE DETECTION METHOD: The RRS reflects unit status to the Operator. The status of the SDS is reflected to the Operator.

COMPENSATING PROVISIONS: The SDS will cause a trip and the reactor will enter a safe condition.

AECB CLASSIFICATION: 2

REMARKS: This failure mode presents a case whereby it is possible for the SDS to trip, caused by an RRS delayed step-back. Although the SDS causes a safe condition to occur, unit power to the grid is lost and the reactor may not be restarted for 8 h. If a step-back had been executed a reactor restart would have been possible in 0.5 h.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-3

NOMENCLATURE: Digital Control Computer Data Link

FUNCTION: The DCCs are connected by a data link which utilizes direct memory access (DMA) to perform the data transfers.

FAILURE MODES AND CAUSES: Faulty hardware could cause inadvertent writing to the memory of the destination DCC. The existing memory protection features will not protect against this as their purpose is to safeguard against software overwriting other software regions. Checksumming may or may not detect the problem, depending on whether the affected memory is checksummed and on how effective the checksum algorithm is at detecting multiple bit failures. If a step-back condition occurs following memory corruption of the receiving DCC, the step back could be prevented, as a unanimous agreement between the DCCs is required.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: The memory of the receiving DCC becomes corrupt.

B. NEXT HIGHER LEVEL: The receiving DCC would fail to make the proper step-back determination, while the sending DCC requests a step-back condition.

C. END EFFECTS: The DCCs would be rendered incapable of effecting a step-back condition.

FAILURE DETECTION METHOD: The SW of the receiving DCC may fail in some manner which is visible. The Operator would note that one DCC has entered the step-back state.

COMPENSATING PROVISIONS: The SDS will shut down the reactor and the reactor will enter a safe condition.

AECB CLASSIFICATION: 1

REMARKS: The probability of the hardware error writing into a wrong location in the destination machine, and the checksum not identifying the fault, and the program continuing to execute, is very low, although technically possible. Further analysis is required to establish actual operational details.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-4

NOMENCLATURE: Digital Control Computer Interrupt System

FUNCTION: The RRS is controlled by dual redundant DCCs. The suite of programs is initiated by a priority interrupt system. The interrupt system not only handles the hardware peripherals via interrupt handlers, but there are a series of timers which trigger programs to be run at certain times. Some of these programs are critical to the correct operation of the reactor regulating, setback, and step-back operations.

The computer has five built-in high priority interrupts: memory protect violation, power fail/restart, memory parity error, watchdog auto-restart, and the real-time clock. There is one system interrupt, the console switch, which is the lowest level interrupt. All other devices interrupt via priority interrupt modules (PIMs). There are three PIMs which handle a maximum of 59 interrupt sources (see Table RRS-4-1). These are split into 27 primary interrupt levels, with five of these levels having eight sublevels each. Refer to Table RRS-4-1 for more detail on the interrupt structure. These PIMs follow the five built in high priority interrupts in the overall structure, and the console switch is the only device which has a lower level interrupt than PIM #3.

All software programs are initiated by timers or by the background executive loop (BEL). The BEL runs when no other program is operating. The remaining programs are divided into two groups. The fast periodic programs run every 0.25-0.50 s, and are initiated by count down register (CDR) #2, which occupies position 20 in the interrupt structure, and is assigned interrupt level 20 (octal). The slow periodic programs are initiated by CDR #6, which occupies position 59 in the interrupt structure, and is assigned interrupt level 27 (octal).

FAILURE MODES AND CAUSES: To initiate the step-back program or the reactor regulating program (fast), the timer CDR #2 must be able to interrupt the processor. The interrupt will be masked out or inhibited by any higher priority level device or interrupt service routine (ISR). Once the SBM program or RRSFST starts to run, it can still be interrupted by a higher priority device.

There are 25 higher level devices, excluding spares, fast periodic stuck function timer, memory protect violation, power fail/restart, memory parity error, watchdog auto-restart, and the real-time clock. These 25 devices include most of the hardware devices such as displays, fixed head disk, moving arm disk, printers, station clock, digital scanner(s), digital I/O, etc. The scanner alone can generate 2,048 interrupts simultaneously when an annunciation switchover occurs. If the system becomes busy, and there are a large number of coincident interrupts, it is possible that CDR #2 will get locked out. Even if the step-back program is allowed to run, it could get interrupted to the extent that it will run very slowly.

OPERATIONAL MODE: Normal, Alternate

# Table RRS-4-1 Priority Interrupt Structure

| Interrupt Number | Interrupt Level (Octal) | Interrupt Sub-level | Description |
|---|---|---|---|
| 1 | 0 | | Sequence of events |
| 2 | 1 | | CDR #7 |
| 3 | 2 | | Remote digital scanner #1 |
| 4 | 3 | | Remote digital scanner #2 (Unit 6 only) |
| 5 | 4 | | FHD transfer complete |
| 6 | 5 | | IOBIC #2 transfer complete |
| 7 | 6 | | Remote data link transfer request |
| 8 | 7 | | IOBIC #1 transfer complete |
| 9 | 10 | 0 | X display error |
| 10 | | 1 | IOBIC #3 display complete |
| 11 | | 2 | Y display error |
| 12 | | 3 | IOBIC #4 display complete |
| 13 | | 4 | Station clock |
| 14 | | 5 | PTR ready |
| 15 | | 6 | CDR #8 |
| 16 | | 7 | Test |
| 17 | 11 | 0 | BIC #2 Statos transfer complete |
| 18 | | 1 | Statos Print Controller Not Busy |
| 19 | | 2 | VHC not busy |
| 20 | | 3 | Alarm acknowledge external interrupt |
| 21 | | 4 | Alarm reset external interrupt |
| 22 | | 5 | Horn silence external interrupt |
| 23 | | 6 | Spare |
| 24 | | 7 | Test |
| 25 | 12 | | BIC #1 MAD transfer complete |
| 26 | 13 | | MAD seek complete |
| 27 | 14 | | Spare |
| 28 | 15 | | Spare |
| 29 | 16 | | Spare |
| 30 | 17 | | CDR #1 Fast Periodic Stuck Function Timer |
| 31 | 20 | | CDR #2 Fast Periodic Function Timer |
| 32 | 21 | 0 | Keyboard #0 |
| 33 | | 1 | Keyboard #1 |
| 34 | | 2 | Keyboard #2 |
| 35 | | 3 | Keyboard #3 |
| 36 | | 4 | Keyboard #4 |
| 37 | | 5 | Keyboard #5 |
| 38 | | 6 | Keyboard #6 |
| 39 | | 7 | Test |
| 40 | 22 | 0 | Keyboard #7 |
| 41 | | 1 | Keyboard #8 (Unit 6 only) |
| 42 | | 2 | Keyboard #9 |
| 43 | | 3 | Hold Reactor |
| 44 | | 4 | Turbine trip |
| 45 | | 5 | Richview Req |
| 46 | | 6 | Richview equalizer (Unit 6 only) |
| 47 | | 7 | Test |
| 48 | 23 | 0 | Alarm acknowledge (Unit 6 only) |
| 49 | | 1 | Alarm reset (Unit 6 only) |
| 50 | | 2 | BIC #5 Printer complete (Unit 6 only) |
| 51 | | 3 | Print controller not busy (Unit 6 only) |
| 52 | | 4 | Spare |
| 53 | | 5 | Spare |
| 54 | | 6 | Spare |
| 55 | | 7 | Test |
| 56 | 24 | | CDR #3 |
| 57 | 25 | | CDR #4 Executive Time Check (EXTC - 0.5s) |
| 58 | 26 | | CDR #5 Slow Periodic Stuck Function Timer |
| 59 | 27 | | CDR #6 Slow Periodic Function Timer |

## FAILURE EFFECTS

A. LOCAL EFFECTS: RRSFST and SBM programs will run slowly and/or will be delayed.

B. NEXT HIGHER LEVEL: In the event of a plant problem, the MCA rod insertion could be delayed.

C. END EFFECTS: If the CDR#2 is locked out or delayed, it is possible that CDR#4 also will be locked out as it has a lower priority. CDR#4 triggers EXTC, which triggers the watchdog. Thus if CDR#2 is locked out for more that 2.5 s, the watchdog will probably timeout and shut down the DCC. Thus the stepback should not be delayed by more than 2.5 s. If the DCC does not shut down the reactor the SDS will do so.

FAILURE DETECTION METHOD: The DCC or SDS would shut the reactor down.

COMPENSATING PROVISIONS: The reactor will shut down into a safe state.

AECB CLASSIFICATION: 2

REMARKS: The computer system is completely built around the priority interrupt structure. There is no central executive in the modern sense, which will allocate resources to the various programs. The timers which initiate the critical programs are set a long way down the priority interrupt chain. It is necessary to set hardware devices which are used by a program at a higher priority level than the program itself. However, with the timer set so low in the chain there must be a significant chance of a delay caused by higher level interrupts.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-5

NOMENCLATURE: Digital Control Computer Software Loading

FUNCTION: The load imposed by the application SW on the Varian V72 CPU. The particular parameter which indicates how busy the CPU becomes, is known as CPU occupancy. As CPU occupancy becomes higher, response time to such things as periodic function requests (Figures RRS-5-1 and RRS-5-2) become longer, as illustrated in Figure RRS-5-3. In addition, as CPU occupancy increases, there is less available capacity to handle additional requirements even if they are of short duration (e.g., scanner interrupts).

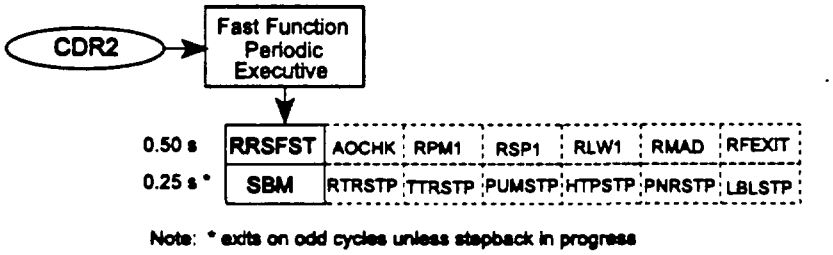


Figure RRS-5-1 Fast Periodic Functions

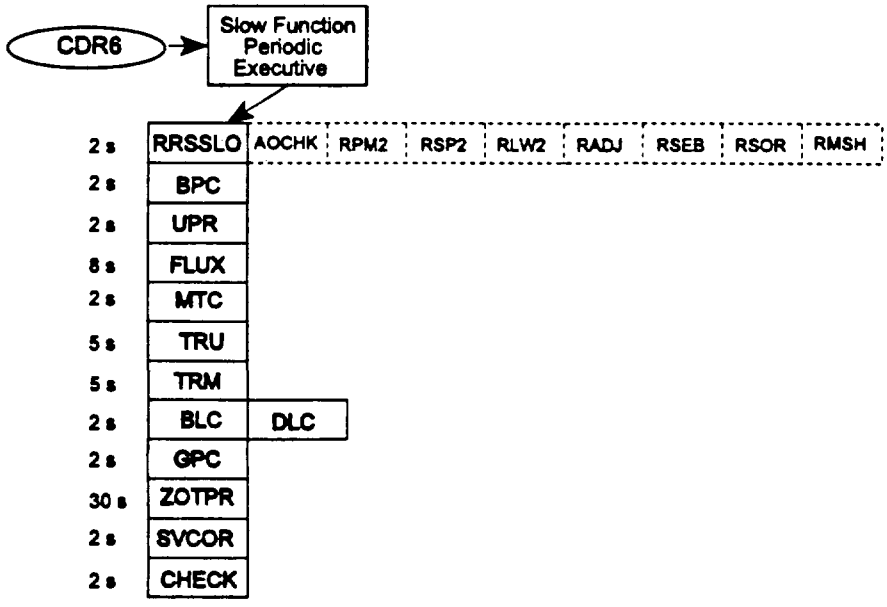


Figure RRS-5-2 Slow Periodic Functions

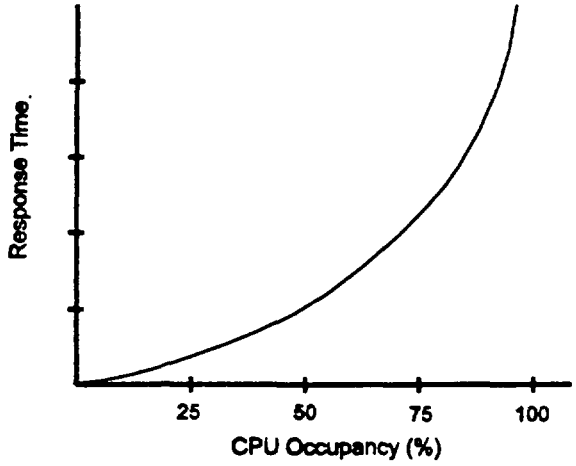


Figure RRS-5-3 Effect of Software Loading

During regular operation (i.e., when a step-back is not taking place), the SBM program executes every 0.25 s, with alternate executions involving no computation. It is uncertain how much of an additional effect a step-back has on CPU occupancy as a result of the SBM performing additional computations during these alternate executions, which are required during a step back involving the drop of the four MCAs.

It is uncertain how much of an additional effect alarm annunciation has on CPU occupancy. CPU occupancy can be severely impacted by the unit contact scanner. SER #B1, A93-143 from Bruce 'A' describes a situation when the SW was not able to tolerate a large number of interrupts from the scanner. The SW now will handle up to 3000 interrupts from the scanner but at an uncertain cost. Perhaps this explains why the internal watchdog time-out is so long (refer to FMEA RRS-10 Watchdog Timer). In addition, Unit 6 DCCs may have an even higher load because of the requirement to service the "sequence of events" scanner.

FAILURE MODES AND CAUSES: If the DCC processors are too busy, their ability to process input data in a timely fashion is impaired. It is possible, given its present very high loading, that under the right conditions the processor will react too slowly to respond properly to a step-back condition.

OPERATIONAL MODE: Normal, Alternate

FAILURE EFFECTS

A. LOCAL EFFECTS: The DCC software will execute too slowly compared with the real-time demands to step back.

B. NEXT HIGHER LEVEL: The DCCs will step back but the step back will be delayed.

C. END EFFECTS: The SDS will respond to the existing conditions faster than the step-back SW.

FAILURE DETECTION METHOD: Operator notes that regulation (i.e., other real-time processing requirements) is lagging behind demands.

COMPENSATING PROVISIONS: The SDS will shut down the rector and the reactor will enter a safe condition.

AECB CLASSIFICATION: 2

REMARKS: During the trip to Bruce 'B', it was revealed that a loading analysis was performed during commissioning. The fixed head disk was replaced by MegaRam, which should not have impacted the loading. Various SW modifications have been made which would have increased the loading slightly from its original value. Presently, Ontario Hydro estimates the CPU occupancy to be between 75% and 95%, probably 85%. Additional SW modifications are pending which will increase the load further. Furthermore, it is understood that the SW loading is going to be measured soon by Ontario Hydro, when the reactor is scheduled to be shut down.

The determination of the actual loading is very important. It is also important to determine how the CPU performance analysis is conducted (e.g., HW data analyser, SW performance monitor). In section 4.1.3, page 4-3, of DM-29-66500-000, it states that "The spare countdown register #7 is temporarily assigned to monitor system loading and is set to interrupt in four milliseconds. This timer can, of course, be disabled if system monitoring is not required."

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-6

NOMENCLATURE: Digital Control Computer/Critical Digital Output Contacts.

FUNCTION: The reactor regulating system is controlled by dual redundant DCCs. The outputs to the plant are driven via analog outputs and digital outputs. The digital outputs are effected via relays. The relays are mercury wetted relays on the DCC circuit card assemblies, and via telephone type relays in the relay equipment racks. There are some critical digital outputs which could cause a reactor shutdown in the event that the relays failed closed. To reduce the chance of this occurring, these critical digital outputs have two relays placed in series, driven by two independent digital outputs on the DCCs.

FAILURE MODES AND CAUSES: If a high surge current passed through the relay contacts, the contacts could weld closed. As the current would pass through both contacts, it is possible that both relays would weld closed at the same time. If only one relay contact were to get stuck closed, there is no function in the system which could detect this. Thus, there would be an undetected failure. A subsequent failure of the second contact would cause an operational failure.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: A control function would continue to operate after the DCC requested the function not operate.

B. NEXT HIGHER LEVEL: A mechanical unit, such as the reactor control rods, could be driven right in or right out.

C. END EFFECTS: Unit power output not available to the grid.

FAILURE DETECTION METHOD: Depends upon the area of the failure. The problem would be detected by the RRS or SDS. The problem would probably be annunciated to the operator.

COMPENSATING PROVISIONS: The RRS or SDS will shut down the reactor and the reactor will enter a safe condition.

AECB CLASSIFICATION: 4

REMARKS: The designers of the system used duplicate relay outputs on all outputs deemed to be critical to the safe operation of the system. However, there is no function in the system which can detect a failed output, and many such faults could exist undetected. A test program applied during reactor shutdown would detect stuck contacts.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-7

NOMENCLATURE: Relay, Control Transfer Frame

FUNCTION: The relays are used to transfer control of critical outputs from the DDC master computer to the DCC slave computer.

FAILURE MODES AND CAUSES: Loss of relay function caused by component failure induced in the wear-out portion of the component life curve.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: Transfer of control from one computer to the other may not be effected.

B. NEXT HIGHER LEVEL: The fault may propagate through to the system level in such a manner that causes an RRS failure, leading to an eventual trip by the SDS.

C.END EFFECTS: Unit power output unavailable to grid.

FAILURE DETECTION METHOD: RRS may announce status to the Operator. SDS trip.

COMPENSATING PROVISIONS: Rod drop by SDS produces a reactor safe condition.

AECB CLASSIFICATION: 4

REMARKS: The relays in question are not sealed, as opposed to the mercury-wetted reed relay type associated with the digital outputs. Although they are drip-proofed, in fact these relays are open to the atmosphere and are exposed to all the effects of corrosion caused by dust, moisture, and gases.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-8

NOMENCLATURE: Digital Control Computer Software Bugs

FUNCTION: DCC SW which is identical in both DCCX and DCCY.

FAILURE MODES AND CAUSES: It is well known that redundancy is beneficial from a HW standpoint, as failures are random in nature. In the case of the DCCs, the benefit gained by using two computer systems instead of one is solely for the benefit of HW redundancy.

SW failures, however, are systematic (i.e., the system will fail every time a particular set of conditions occur). Within safety-critical sectors, such as nuclear power generation, this knowledge has given impetus to using N-version programming techniques, in which the HW, SW (firmware, application SW, operating system, compilers, libraries, etc.), tools, development personnel, and management are different between the N versions, where N is usually 3. In this case, redundancy in SW takes the form of diversity. The use of this approach comes with its own set of technical problems and, of course, high cost. In the case of DCCs, N-version programming typically has not been addressed because these systems have not been considered to be safety-critical, even though they control the reactor, turbine, and boiler.

It does not require a common cause failure analysis (CCFA) to identify that the SW which resides in the DCCs is an obvious potential source of problems, which could result in failure to step back, other step-back problems, or a host of other problems.

SW exhibits what is known as "weak link" behaviour, in which failures in even the unimportant parts of the code can have unexpected repercussions elsewhere. Errors also are more common, more pervasive, and more troublesome in SW than in other technologies. Even trivial clerical errors can have major consequences.

As the SW is identical between DCCs X and Y, errors within specification, design, and implementation of the SW can result in dual processor failure.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: Unknown errors.

B. NEXT HIGHER LEVEL: Unknown failures.

C. END EFFECTS: Potential step-back problems, occurring under unusual situations, which could cause failure to step-back, incomplete step-back, etc.

FAILURE DETECTION METHOD: Depends upon how the SW has failed.

COMPENSATING PROVISIONS: The SDS will shut down the reactor and the reactor will enter a safe condition.

AECB CLASSIFICATION: 1

REMARKS:

1. Importance of SERs

Although the SERs are a useful source of information regarding mishaps that have occurred in the past, they are of limited comfort with respect to the potential existence of yet-undiscovered SW problems. All too often, problems within SW which cause the system to malfunction in a serious manner have existed for some period, whether it is months or years. The catalyst that is required to bring these errors to the surface typically is a particular, although unusual, event or combination of events (i.e., an uncommon input trajectory).

2. Importance of testing

The sofware at Bruce 'B' has been in operation for many years and has been tested exhaustively. It should be noted that:

a. Many SW errors in industry have gone undetected using standard verification and validation procedures. It is common to find serious flaws even within SW which has been subjected to a thorough and disciplined testing regime.

b. It is recognized that if SW behaves correctly under a large set of test cases, the only accurate statement one can make is that the SW is not known not to work (i.e., testing can show the presence of bugs but cannot show that the SW is free of errors).

c. Problems which are discovered by testing are usually of the type which do not typically cause serious malfunctions in the future.

3. Weaknesses of Assembly language

This type of language is the lowest level possible. At one time, Assembly language was the only available choice and it was required because of limited physical address space and processor speed. Typically, it is no longer recommended within SW engineering and SW safety standards (refer to Table RRS-8-1) because of its error-prone nature, lengthy coding time, and lack of protection offered by the language and the assembler. Structured, strongly-typed programming languages are now preferred, especially for mission- or safety-critical SW [Evaluating software..., 1994]. Other shortcomings of this type of language are the lack of supporting tools, such as static (e.g., McCabe, Cadre tools) and dynamic code analysers, and the lack of available expertise on the market. It is recognized that when Bruce 'B' was implemented, assembly language was probably the only choice of language available.

Table RRS-8-1 Programming Language Preference According to IEC DIS TC 65A

| Language | SIL1 | SIL2 | SIL3 | SIL4 |
|---|---|---|---|---|
| Ada | HR | HR | R | R |
| Ada Subset | | | HR | HR |
| Modula-2 | HR | HR | R | R |
| Modula-2 Subset | | | HR | HR |
| Pascal | HR | HR | R | R |
| Pascal Subset | | | HR | HR |
| Fortran 77 | R | R | R | R |
| Fortran 77 Subset | | | HR | HR |
| C | -- | -- | NR | NR |
| C Subset | | | R* | R* |
| PL/M | R | R | NR | NR |
| PL/M Subset | | | R* | R* |
| BASIC | -- | NR | NR | NR |
| Assembler | R | R | -- | -- |
| Assembler Subset | | | R* | R* |

Notes:

SIL Safety Integrity Level, for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems. SIL4 has the highest level of safety integrity, SIL1 has the lowest.

HR Highly Recommended for this safety integrity level.

R Recommended for this safety integrity level.

— No recommendation for or against being used for this safety integrity level.

NR Not Recommended for this safety integrity level.

* A precise set of coding standards is required, in addition to the use of the subset.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-9

NOMENCLATURE: Digital Control Computer Annunciation System (priority level)

FUNCTION: The reactor regulating system is controlled by dual redundant DCCs. The annunciation system receives messages from running programs, it scans some analog inputs, it receives messages from the channel outlet temperature monitor, and it receives digital input data from the scanner.

FAILURE MODES AND CAUSES: The annunciation system relies on the background loop to display messages. This loop, under severe loading condition, may not run for up to 25 s. Annunciation messages to both the CRTs and printers will be delayed.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: A plant problem would not get annunciated in a timely manner on the CRT or printer.

B. NEXT HIGHER LEVEL: The reactor regulating system may shut the system down, although the operators may have been able to control the situation if they had been alerted to the problem.

C. END EFFECTS: The reactor shut-down system, or the reactor regulating system, would eventually shut down the system.

FAILURE DETECTION METHOD: The DCC would correct the problem.

COMPENSATING PROVISIONS: DCC would continue to control the reactor and set it to a safe condition. The hard-wired windows may annunciate the problem.

AECB CLASSIFICATION: N/A, production issue.

REMARKS: The annunciation system has been given a very low system priority. With respect to safety, the operator is not credited for 15 minutes, so the DCC would shut down the reactor and put it in a safe mode.

FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-10

NOMENCLATURE: Digital Control Computer Watchdog Timer

FUNCTION: Two watchdog timers are used per DCC. The contacts of the two timers are connected in series, such that a failure of either watchdog will cause a transfer of control to the other DCC (Figure RRS-10-1). Via hardware components, the watchdog timer time-out is set at 2.5 s. Within the SW, though, there is an additional watchdog time-out of 25 s.

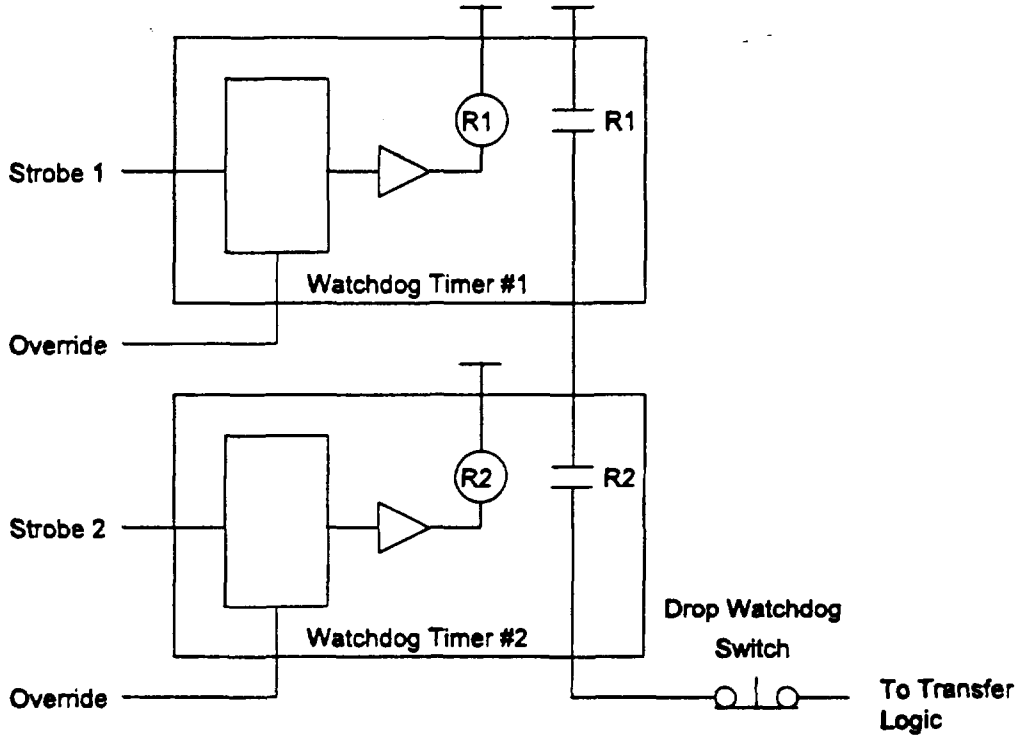


Figure RRS-10-1. Watchdog Timer Circuit

The Executive Time Check (EXTC) runs every 0.5 s. A SW counter, called OPMON, is checked by EXTC. If OPMON is not zero, it is incremented by one and the watchdog timer is reset to prevent it from timing out. If the watchdog timer times out, all digital outputs, including the interlock relays, are opened to isolate this DCC and connect the other DCC to the field. Within the background executive loop, OPMON is set to -50. If OPMON reaches 0, (i.e., 25 s have elapsed since the last execution of the background executive loop), 2.5 s later the watchdog timer will drop out. Therefore, a total of 27.5 s must elapse before the watchdog timer will drop out if the DCC SW fails such that the background executive loop is not executed.

FAILURE MODES AND CAUSES: 27.5 s is an inordinately high value for this time-out. Implementing the watchdog time-out in this manner indicates that there are times when the processor legitimately is expected to be almost too busy to service the background executive loop. Otherwise, OPMON would be set to a more reasonable value. Perhaps this is an attempt to mask the effect of temporary high loading conditions, such as in the case of a large number of scanner interrupts (refer to SER #B1, A93-143). Refer to FMEA RRS-5, Software Loading.

OPERATIONAL MODE: Normal, Alternate

FAILURE EFFECTS

A. LOCAL EFFECTS: Certain classes of software or hardware faults could result in a 27.5-s watchdog timeout.

B. NEXT HIGHER LEVEL: The watchdog timer contacts, associated with the impaired DCC, close following a lengthy delay.

C. END EFFECTS: Control will transfer to the other DCC. The impared DCC will be restarted.

FAILURE DETECTION METHOD: The problem would be annunciated to the operator.

COMPENSATING PROVISIONS: The SDS will shut down the reactor and the reactor will enter a safe condition.

AECB CLASSIFICATION: 2

REMARKS: If the reason for the value of OPMON being set so high is to compensate for scanner interrupts, it makes more sense to:

- either throttle the interrupts in some way; or
- sense the scanner problem and only set OPMON to a high value for that situation, restoring it back later to a more reasonable value.

If scanner interrupts are not the reason for the high value of OPMON and the value needs to be set this high, it demonstrates that the processor is too heavily loaded.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-11

NOMENCLATURE: Shut Down System/RRS Interactions

FUNCTION: The RRS is controlled by dual redundant DCCs. The DCCs are intended to control the reactor and associated systems, such that the various elements work together and the power level of the reactor is at the required level, as set by the operator or the demand on the turbine. The reactor regulating system provides the fine control over the reactor power and the step-back system will reduce the reactor power rapidly if various upset conditions occur. If the DCCs fail to act in a timely manner, there are two SDSs monitoring the reactor, and one or both of these can shut down the reactor.

FAILURE MODES AND CAUSES: The SDSs and the DCCs monitor different parameters in the reactor and turbine system. They also use different monitoring devices, which are the subject of different calibration errors. It is conceivable that the SDSs could detect a fault which the DCCs would not detect, or would detect at a later time than the SDSs. One such condition has been noted in the Bruce 'B' safety report (AECB ISN 25945) relating to heat transport system oscillations (section 3.3.5.5.2.2). Other such conditions may exist but may be undetected.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: The SDS(s) will operate.

B. NEXT HIGHER LEVEL: The reactor will shut down.

C. END EFFECTS: No power will be provided to the grid.

FAILURE DETECTION METHOD: Annunciation via the DCCs and the hard-wired windows.

COMPENSATING PROVISIONS: The SDSs will put the reactor in a safe condition.

AECB CLASSIFICATION: N/A, production issue only.

REMARKS: To further analyse this failure scenario, much more detail on the reactor system would be required than can be provided within the scope of this contract.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-12

NOMENCLATURE: Digital Control Computer Step-back Monitor

FUNCTION: The reactor regulating system is controlled by dual redundant DCCs. There is a step-back monitor (SBM) program which monitors seven critical parameters in the system and initiates a power step back if any of these parameters go out of allowable, preset ranges. The program may set the power back to zero (shutdown) or to some intermediate level. The method of initiating a step back is to release the clutches on four mechanical control absorber rods. These rods drop into the core to absorb neutrons and reduce the reactor power. The SBM can reactivate the clutches and, thus, can catch the rods if it determines that the original fault condition has cleared, or if the reactor power level has fallen below the step-back power set point.

FAILURE MODES AND CAUSES: Once a step back is in progress, the SBM only monitors the power level and the one parameter that initiated the step back. The program will stop the step back if the power has fallen below the predefined step-back level OR if the parameter which caused the step back is now within tolerance. Once a step back has been initiated, the program does not check the other six parameters which it normally checks. If the power has fallen below the preset step-back level or if the original parameter is now in limits, the step back is halted, even if other parameters are now out of their preset limits.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: The MCA rods would initially start to drop but they would be caught when partially inserted.

B. NEXT HIGHER LEVEL: The reactor power initially would fall but then stabilize at an intermediate level.

C. END EFFECTS: The reactor shut-down system, or the reactor regulating system, would eventually shut down the system.

FAILURE DETECTION METHOD: The RRS would detect that there was a problem on its next cycle and reinitiate the rod drop. The SDS may detect the problem first and shut down the reactor independently.

COMPENSATING PROVISIONS: The RRS or the SDS will shut down the reactor and the reactor will enter a safe condition.

AECB CLASSIFICATION: 3

REMARKS: Before the SBM is permitted to catch the rods, it should ensure that all seven critical parameters are within safe limits.

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

IDENTIFICATION NUMBER: RRS-13

NOMENCLATURE: Digital Control Computer CHECK Program

FUNCTION: The computer self-check program, CHECK, is invoked by the slow periodic function executive. CHECK is an unswitched function which is executed every 2 s. Six failure detection functions performed by CHECK are of prime importance in that "no other system check exists for the same fault". These functions are: (1) CPU instruction test, (2) digital I/O test, (3) transfer of control digital output test, (4) Buffer Input/Output Controller (BIOC) data paths test, (5) analog input test for critical chassis, and (6) integrity test (by checksums) of certain parts of the executive and the step-back routine.

FAILURE MODES AND CAUSES: If a hardware failure occurs, which goes undetected by CHECK's diagnostics, this could cause the SBM to make incorrect decisions. If a step-back situation is required but SBM, within the affected DCC, fails to make the determination, the step back would be prevented as a unanimous agreement between DCCs is required. For instance, the instruction test apparently performs a comprehensive arithmetic instruction test using all possible arithmetic functions and the fixed code check performs checksums (only single-bit detection appears possible) on all resident programs. If the coverage awarded by these programs is insufficient, a step-back could be prevented.

OPERATIONAL MODE: Normal, Alternate

## FAILURE EFFECTS

A. LOCAL EFFECTS: Inaccurate calculations or corrupted control flow in the SBM program would not be detected.

B. NEXT HIGHER LEVEL: The affected DCC would continue to operate while the other DCC requests a step-back condition.

C. END EFFECTS: The DCCs would be rendered incapable of effecting a step-back condition.

FAILURE DETECTION METHOD: Other software may fail causing a transfer of control to the other DCC. The operator would note that one DCC has entered the step-back state.

COMPENSATING PROVISIONS: The SDS will shut down the reactor and the reactor will enter a safe condition.

AECB CLASSIFICATION: 1

REMARKS: As the documentation supplied regarding CHECK is so sparse but its function is so important, further investigation into the CHECK program's coverage is required (e.g., details of instruction tests, algorithm used for checksumming) for a thorough evaluation of CHECK.

SUPPLEMENTARY INFORMATION:

1. If a checksum error occurs, it appears that it is only annunciated.

2. It is believed that a report is available from AECB regarding self-testing in general.

APPENDIX B

# DETAILED ANALYSIS OF RELIABILITY MODELLING

## B.1 System Availability Requirement

In document DD-29-66400-1, there is an expectation of Bruce 'B' DCC availability in excess of 99% per DCC, i.e., less than a downtime of 87.6 h/year per DCC. Also, it is indicated that prior experience with similar systems has shown forced unit outages of 8 h/year due to computer faults. Therefore, it is assumed that at Bruce 'B' the DCC computers should cause less than 8 h/year of unit outage. Assuming Bruce 'B' DCCs each have an availability of at least 99%, when used in a redundant pair configuration, the availability should be 99.99%, or a downtime of 0.876 h/year. Thus the forced unit outage due to a dual DDC failure can be expected to be less than 1.0 h/year.

What follows is a theoretical analysis of what the failure expectation would be on the present Bruce 'B' DCCs.

## B.2 Hardware Prediction

The RRS electronics, except for peripheral equipment such as CRT display monitors, keyboards, and printers, is mounted in either steel cabinets or on frames, as shown in Table B-1.

Table B-1. Electronic Contents of Cabinets or Frames

| Cabinet/Frame | Contents |
|---|---|
| XS1, XS2, YSI, YS2 | Analogue Input System |
| XS3, YS3 | Computer |
| | Fixed Head disk |
| | Moving Head Disk |
| | Paper Tape system |
| | Interrupt Chassis with PIMS and |
| WDT#2 | |
| XS4,YS4 | Display Controller |
| | Digital Output System |
| | Video Mux |
| XS5, YS5 | Analogue Output |
| | Digital Input |
| | Countdown Registers, WDT#1, Scanner |
| Interface | |
| Scanner#1 | Scanner Assemblies |
| Scanner#2 | Scanner Assemblies |
| Transfer Logic | Relays |
| Control Distribution | Wire Terminations |

For the generation of electronics of which the RRS is assumed to be typical, it can be expected that there will be an average of one failure per cabinet/frame per year [Assessment of..., 1994]. Therefore, about 14 failures/year can be expected to occur in the cabinet/frame electronics. With respect to peripherals, the keyboards generally have a very high MTBF and can be expected to contribute 1 failure/year. In addition, 1 failure/year can be expected to be contributed from the displays and printers. Note that most failures associated with displays and printers are of the wear-out variety and random failures are relatively infrequent, as equipment can be replaced "on condition" as deterioration is noted.

Overall, it can be expected that about 17 failures/year may occur in the RRS electronics. Assuming that the RRS X, Y electronics is symmetrical, about 8.5 failures/year can be expected for each of the RRS X, Y complement.

## B.3 Software Prediction

Work documented in Musa et al. [1990] demonstrates that it is possible to model software in useful ways that can allow reasonable predictions of software reliability to be made. Basically, a model is selected and is used to calculate the execution time failure rate and then this rate is converted to calendar time, bearing in mind the particular approach taken to testing. For this purpose the Basic Execution Time (BET) model has been applied, as it is most suitable for predictions. All of the the models depend on a variety of factors that have been identified as impacting software reliability, particularly, the number of source lines of code statements (SLOCs), processor speed, processor utilization (loading), and others.

### B.3.1 Execution time component

SLOCs can be computed as shown in Table B-2, which is expressed in thousands of SLOCs (KSLOCs).

The cycle time of the processor is 660 ns and, therefore, the processor speed is 1.52 MHz. Processor loading is estimated to be approximately 85%. The inherent faults, $\omega_0$, can be calculated as:

$$\omega_0 = \omega_I . \Delta I$$

$$= (1.48/1000)\ 65{,}000 = 96.2 \text{ faults}$$

where $\omega_I$ is inherent faults per source instruction, with the average given in Musa et al. [1990] as 1.48/KSLOCs at operation (commissioning), and $\Delta I$ is the number of lines of executable source code.

The total number of failures expected, $v_0$, is given by:

$$v_0 = \omega_0 / B = 96.2/0.955 = 100.7 \text{ faults}$$

where $B$ is the fault reduction factor and is given by Musa et al. [1990] as an average of 0.955.

Table B-2. RRS Module vs. KSLOCs

| RRS Module | KSLOCs |
|---|---|
| Executive: | 11.0 |
| Control Programs: | |
| BLC/DLC | 14.0 |
| ZOTPR | 4.0 |
| UPR | 7.2 |
| BPC | 2.5 |
| CHECK | 4.2 |
| TRU | 5.7 |
| GPC | 2.5 |
| FLUX | 6.2 |
| RRSSLO | 5.5 |
| RRSFST+SBM | 2.2 |
| Total | 65.0 |

The number of executable object instructions, $I$, is given by:

$$I = \Delta I . Q_X = 65{,}000 \text{ instructions (inst)}$$

where $Q_X$ is the code expansion ratio and equals 1.0, as the code is written in assembler. The linear execution frequency, $f$, is given by:

$$f = r / I$$

$$= (1.52 \times 10E6 \text{ CPU inst/s})/(0.065 \times 10E6 \text{ inst}) = 23.4 \text{ cycles/CPU s}$$

where $r$ is the average object execution rate. The initial unadjusted failure intensity, $\lambda_{0u}$, can be computed from:

$$\lambda_{0u} = f . K . \omega_0 = 23.4 \ (4.2 \times 10E\text{-}7) \ 96.2$$

$$= 0.945 \times 10E\text{-}3 \text{ failures/CPU s or } = 3.40 \text{ failures/CPU h}$$

where $K$ is the fault exposure ratio, which is given in Musa et al. [1990] as an average of 4.2 x 10E-7.

Finally, an adjustment is required to account for the processor loading, $L$, of 85% and is applied as follows to arrive at initial failure intensity :

$$\lambda_0 = \lambda_{0u} . L$$

$$3.40 \times 0.85 = 2.89 \text{ failures/CPU h}$$

The initial software MTBF, $MTBF_0$ is, therefore:

$$MTBF_0 = 1/\lambda_0 = 1/2.89 = 0.34 \text{ h}$$

This concludes the execution time portion of the calculation and now this result will be converted into the more familiar calendar time.

### B.3.2 Calendar time component

In calculating the initial software MTBF, it was assumed that the software was delivered for use at the beginning of operation (commissioning). Suppose it is desired to improve the MTBF to at least six months (8760/2) 4380 h, i.e., by a factor of (4380/0.34) 12,882. This improvement will require further effort, based on fault detection, isolation, correction, and testing.

The additional CPU hours, $\Delta\tau$, required can be computed from:

$$\Delta\tau = [\nu_0/\lambda_0] / \ln [\lambda_P/\lambda_F]$$

$$= (100.7/2.89) \ln 12{,}882 = 329.7 \text{ CPU h}$$

where $\lambda_P$ is the present failure intensity and $\lambda_F$ is the failure intensity objective.

The additional 329.7 CPU h can be related to calendar time, via a calendar time to execution time ratio. The ratio development proceeds on the basis of a debugging model developed by Musa et al. [1990], which takes into account:

a. Resources (people, machines, etc.) used in operating the program for a given execution time and processing an associated quantity of failures.

b. Resource quantities available.

c. The degree to which a resource can be utilized (due to bottlenecks) during the period in which it is limiting.

A typical scenario is as follows. At the start of testing a large number of failures are discovered, separated by short time intervals. Testing activity is slowed significantly, or even stopped, to let the people who are fixing the faults keep up with the load. The failure correction team has become the bottleneck. As testing progresses, the interval between failures becomes longer and longer. The time of the failure correction personnel is no longer filled with failure correction work. The test team has become the bottleneck. The effort required to run tests and analyse results occupies all of their time. Finally, at even longer intervals, computing resources become limiting.

To be effective, the debugging model requires considerable amounts of detailed information, which is nearly impossible even to estimate at this point in time as the RRS software was developed

essentially over 10 years ago. The inputs required for each of the three limiting phases includes knowledge with respect the following resources: number of failure identification personnel, number of failure correction personnel, and CPU execution time. For each of these resources, the resource utilization also must be known. However, it is expected that calendar time would be of the order of 6 to 12 months.

To overcome the above difficulties, advantage can be taken of the fact that it can be safely assumed that the RRS software has essentially been under continuous debugging for over 10 years. Also, it can be safely assumed that the software is operating in the computer execution time limitation phase, so that failures have a long failure interval. The earlier calculation shows that the the software can exhibit MTBFs in the thousands of hours, provided that the debugging effort involved at least 329.7 CPU h. That this has certainly taken place is without question.

Based on the above, it is expected that the RRS software should exhibit about 1-2 failures/year.

## B.4 System Reliability Prediction

For X, Y segments combined, it can be expected that hardware (17 failures) and software (4 failures) together will contribute about 21 failures, or an average of 10.5 failures/segment/ year. However, practically none of these failures will propagate through to the RRS system level and result in unit outage, as the system is fault tolerant. An estimate of the system MTBF(s) can be derived on the basis of the MTBF and MTTR of the segments. The segment MTBF is 8760/10.5 = 834.2 h. The MTTR is assumed to be of the order of 4 hours. From these parameters, the system MTBF can be calculated as follows [Rau, 1970]:

$$MTBF = (3\lambda + \mu)/ 2\lambda^2$$

$$= (3 \times 1.2 \times 10E\text{-}3 + 0.25)/(1.2 \times 10E\text{-}3)^2 = 176{,}000 \text{ h},$$

where $\lambda$ is the failure rate (1/MTBF), and $\mu$ is the repair rate (1/MTTR).

This very large result, 176,000/8,760 = 20.09 years, is optimistic because the calculation assumes a perfect switchover mechanism and does not account for uncovered faults. On the other hand, not all failures will result in a transfer of control, particularly in the case of peripherals such as keyboards, displays and printers. The system can be modelled more accurately with a Markov [Ibe et al., 1989] approach but the ready result above shows that the MTBF(s) should certainly be on the order of at least several years.

## B.5 Summary

At Bruce 'B' there are four operational units and, assuming a single unit outage of 20 years, it can be expected that there will be a unit outage due to an RRS failure about every five years at that site.

The RRS associated with each unit can be expected to sustain about 21 failures/year, essentially all of which should be masked due to the fault tolerant design of the system and, therefore, appear to be transparent at the system level. However, these failures will lead to maintenance activities such as circuit card replacement, manual computer restart, etc.

APPENDIX C

# DETAILED ANALYSIS OF SIGNIFICANT EVENT REPORTS

AECB provided a total of 141 significant event reports (SERs) relating to computer stalls in the reactor regulating system (RRS) in the form of computer listings. SERs for the last five years were obtained for detailed review.

The SERs were analysed and a failure cause was determined, when possible, for each SER. The designation 'Not Specified' is used when the root cause of the failure could not be determined from the data provided by the AECB. The data was put in a database which was sorted by date and by location. The data is shown in Tables C-1 and C-2.

Table C-1 lists all SERs sorted by date. The last entry in the table is a summary of the failure modes, with the total expressed as a percentage of the total failures.

Table C-2 lists the same SERs sorted by location. This table shows that Bruce 'B' has a very low number of SERs compared with other plants.

Table C.1 SER Analysis Sorted by Date Sheet 1 of 4.

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Spec-ified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Periph-eral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| P3,A82-025 | 820305 | S | 1 | | | | | | | | | | | | | |
| B4,A82-046 | 820510 | S | | | | 1 | | | | | | | | | | |
| B4,A82-067 | 820604 | S | | 1 | | | | | | | | | | | | |
| P3,A82-128 | 821005 | S | | 1 | | | | | | | | | | | | |
| P1,A82-134 | 821010 | S | | | | | | | | | | | | | 1 | |
| L1,82-820 | 821101 | S | | | | | | | | | | | | | 1 | 1 |
| L1,82-040 | 821102 | S | | | | | 1 | | | | | | | | | |
| G2,82-814 | 821115 | S | | | 1 | | | | | | | | | | | 1 |
| P5,B82-163 | 821121 | S | | | | | 1 | | | | | | | | | |
| P5,B82-177 | 821202 | S | 1 | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| L1,83-002 | 830104 | S | 1 | | | | | | | | | | | | | |
| P4,A83-012 | 830210 | S | 1 | | | | | | | | | | | | | |
| G2,83-510 | 830215 | S | 1 | | | | | | | | | | | | 2 | |
| L1,83-009 | 830228 | S | | | | | | 1 | | | | | | | | |
| L1,83-534 | 830301 | S | 1 | | | | | | | | | | | | | |
| L1,83-535 | 830301 | S | 1 | | | | | | | | | | | | | |
| L1,83-641 | 830401 | S | | | 1 | | | | | | | | | | | |
| G2,83-606 | 830601 | S | | | | | | | | | 1 | | | | | |
| P4,A83-072 | 830625 | D | 1 | | | | | | | | | | | | | |
| L1,83-605 | 830628 | S | | | | | | 1 | | | | | | | | |
| L1,83-728 | 830701 | S | | 1 | | 1 | | 2 | | | | | | | | |
| P3,A83-158 | 830912 | S | | | | | | | | | | | | | | 1 |
| G2,83-707 | 830913 | S | 1 | | | | | | 1 | | | | | | | 1 |
| P3,A83-105 | 830925 | D | | | | | | | | 1 | | | | | | |
| L1,83-829 | 831015 | S | | | | | | 1 | | | 1 | | | | | |
| G2,83-814 | 831016 | S | | | | | | | | 1 | | | | | | |
| P1,A83-120 | 831016 | S | | 1 | | | | | | | | | | | | |
| P1,A83-123 | 831018 | S | | | | | 1 | | | | | | | | | |
| G2,83-815 | 831021 | S | | | | | | | | | | | | | | 1 |
| P1,A83-134 | 831027 | S | | | 1 | | | | | | | | | | | |
| P2,A83-133 | 831029 | D | 1 | | | | | | | | | | | | | |
| L1,83-828 | 831030 | S | 1 | | | | | | | | | | | | | |
| G2,83-817 | 831102 | S | | | | | | | 1 | | | | | | | |
| P4,A83-138 | 831113 | S | 1 | | | | | | | | | | | | | |
| P4,A83-999 | 831114 | S | 1 | | | | | | | | | | | | | |
| P4,A83-144 | 831116 | S | 1 | | | | | | | | | | | | | |
| G2,83-016 | 831202 | S | | | | | | | | | | | | | | 1 |
| P1,A83-149 | 831216 | D | 1 | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| P1,A84-001 | 840105 | D | 1 | | | | | | | | | | | | | |

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Spec-ified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Periph-eral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| G2,84-501 | 840115 | S | | | | | | | | | | | | | | 1 |
| P2,A84-002 | 840118 | D | 1 | | | | | | | | | | | | | |
| P5,B84-036 | 840216 | S | 1 | | | | | | | | | | | | | |
| P1,A84-019 | 840301 | D | 1 | | | | | | | | | | | | | |
| P1,A84-026 | 840314 | D | 1 | | | | | | | | | | | | | |
| B3,A84-030 | 840323 | S | | | | | | | | | 1 | | | | | |
| B3,A84-031 | 840324 | S | | 1 | | | | | | | | | | | | |
| G2,84-615 | 840427 | S | 2 | | | | | | | | | | | | | |
| L1,84-611 | 840513 | S | | | | | | | | | | 1 | | | | |
| L1,84-627 | 840515 | S | 1 | | | | | | | | | | | | | |
| L1,84-628 | 840515 | S | 1 | | | | | | | | | | | | | |
| L1,84-605 | 840522 | S | | | | | 1 | | | | | | | | | |
| G2,84-709 | 840731 | S | | | | | | | | 1 | | | | | | |
| B1,A84-083 | 840920 | S | | | | | | | | 1 | | | | | | |
| B2,A84-092 | 841015 | D | | | | | 1 | | | | | | | | | |
| G2,84-809 | 841017 | S | 1 | | | | | | | | | | | | | |
| L1,84-804 | 841022 | S | | | | | | | | | | | | | | 1 |
| L1,84-824 | 841101 | S | 1 | | | | | | | | | | | | | |
| P4,A84-131 | 841112 | S | | | | | 1 | | | | | | | | | |
| G2,84-810 | 841202 | S | | | | | 1 | | | | | | | | | |
| G2,84-811 | 841205 | S | | | | | | | | | | | | 1 | | |
| | | | | | | | | | | | | | | | | |
| B2,A85-006 | 850111 | S | | | | | 1 | | | | | | | | | |
| G2,85-504 | 851117 | S | | | | | | | | 1 | | | | | 1 | |
| P4,A85-079 | 850310 | S | | | | 1 | | | | | | | | | | |
| G2,85-612 | 850413 | S | | | | | | | | | | | 1 | | | |
| L1,85-631 | 850501 | S | 1 | | | | | | | | 2 | | | | | |
| L1,85-603 | 850513 | S | | 1 | | | | | | | | | | | | |
| L1,85-605 | 850515 | S | | | | | | | | | | | | | 1 | |
| B3,A85-064 | 850518 | S | | | | | 1 | | | | | | | | | |
| G2,85-613 | 850524 | S | | | | | | | | | | | | 1 | | |
| L1,85-606 | 850615 | S | | | 1 | | | | 1 | | | | | | | |
| L1,85-604 | 850628 | S | | | | | | | | | | 1 | | | | |
| L1,85-725 | 850801 | S | 1 | | | | | | | | | | | | | |
| B4,A85-108 | 850823 | S | | | | | | | | 1 | | | | | | 1 |
| G2,85-708 | 850910 | S | | | | | | | | 2 | | | | | | |
| P3,A85-110 | 851101 | S | | | | | | | | 1 | | | | | | |
| L1,85-821 | 851115 | S | | | | | | | | | 1 | 1 | | | | |
| G2,85-816 | 851230 | S | | | | | | 1 | | 1 | 1 | | | | 1 | |
| | | | | | | | | | | | | | | | | |
| B7,B86-011 | 860203 | S | | | | | | | | | | | | | 1 | |

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Spec-ified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Periph-eral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| L1,86-532 | 860301 | S | | | | 2 | | | | | 2 | 1 | | | | |
| G2,86-506 | 860311 | S | | | | | 1 | | | | | | | | | |
| L1,86-503 | 860329 | S | | | | | | | | | | 1 | | | | |
| B7,B86-034 | 860401 | S | | | | | | | | | 1 | | | | | |
| L1,86-633 | 860601 | S | 1 | | | | | | | | | | | | | |
| B7,B86-048 | 860602 | S | | | | | | | | | | | | | 1 | |
| P3,A86-105 | 860704 | D | | | | | | | | | | 1 | | | | |
| L1,86-603 | 860605 | S | | | | | | | | | | | | | | 1 |
| L1,86-705 | 860730 | S | | | | | | | | 1 | | | | | | |
| P8,B86-175 | 860825 | S | 1 | | | | | | | | | | | | | |
| P1,A86-141 | 860923 | S | 1 | | | | | | | | | | | | | |
| L1,86-829 | 861101 | S | | | | | | | | | 1 | | | | | |
| B8,B86-074 | 861105 | S | | | 1 | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| P4,A87-009 | 870119 | S | | | | | | | | | | | | | 1 | |
| P4,A87-011 | 870120 | S | | | | | 1 | | | | | | | | | |
| P3,A87-083 | 870525 | D | | | | | | | | | | | | 1 | | |
| P3,A87-084 | 870525 | D | 1 | | | | | | | | | | | | | |
| B1,A87-047 | 870617 | D | | | | | 1 | | | | | | | | | |
| B4,A87-051 | 870624 | S | | 1 | | | | | | | | | | | | |
| P5,B87-112 | 870825 | D | | | | | | | 1 | | | | | | | |
| P18,B87-113 | 870825 | D | 1 | 1 | | | | | | | | | | | | |
| P3,A87-179 | 870829 | D | 1 | | | | | | | | | | | | | |
| P3,A87-184 | 870901 | S | 1 | | | | | | | | | | | | | |
| L1,87-009 | 871007 | S | | 1 | | | | | | | | | | | | |
| B2,A87-079 | 871010 | D | | 1 | | | | | | | | | | | | |
| P3,A87-210 | 871025 | S | | | | | | | | 1 | | | | | | |
| P1,A87-222 | 871115 | S | 1 | | | | | | | | | | | | | |
| P4,A87-229 | 871119 | S | | | | | | | | | | | | | 1 | |
| P3,A87-236 | 871202 | S | | | | | | | 1 | | | | | | | |
| | | | | | | | | | | | | | | | | |
| B3,A88-009 | 880128 | S | | | | | | | | 1 | | | | | | |
| P1,A88-045 | 880228 | D | 1 | | | | | | | | | | | | | |
| L1,88-110 | 880417 | S | | | | | | | | 1 | | | | | | |
| P4,A88-122 | 880707 | S | | | 1 | | | | | | 1 | | | | | |
| B4,A88-090 | 880815 | S | | 1 | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| B1,A89-025 | 890309 | D | | | | | 1 | | | | | | | | | |
| B4,A89-033 | 890327 | S | | | | | | | | | 1 | | | | | |
| B2,A89-053 | 890419 | S | | | | | | | | | | 1 | | | | |
| P3,A89-096 | 890707 | D | | | | 1 | | | | | | | | | | |

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Spec-ified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Periph-eral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| P5,B89-080 | 890728 | S | | 1 | | | | | | | | | | | | |
| P3,A89-105 | 890806 | D | 1 | | | | | | | | | | | | | |
| P3,A89-140 | 891002 | D | | | | | | | | | | 1 | | | 1 | |
| D2,A89-042 | 891217 | D | | 1 | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| B6,B90-007 | 900206 | S | | | | | | | | | | | | | | 1 |
| D2,A90-008 | 900214 | D | 1 | | | | | | | | | | | | | |
| D2,90-024 | 900523 | S | | | | | 1 | | | | | | | | | |
| B4,A90-099 | 900912 | D | | | | | | | | 1 | | | | | | |
| P6,B90-163 | 900914 | S | | | | 1 | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| P1,A91-033 | 910302 | D | 1 | | | | | | | | | | | | | |
| B8,B91-028 | 910315 | S | | | | | | | | | 1 | | | | | |
| G2,91-13 | 910405 | D | | | 1 | | | | | | | | | | | |
| P8,B91-079 | 910621 | S | | | | | | | | | 1 | | | | | |
| G2,91-122 | 910711 | S | | 1 | | | | | | 1 | | | | | | |
| P8,B91-088 | 910804 | S | 1 | | | | | | | | | | | | | |
| P7,B91-091 | 910827 | S | | | | | | | | | 1 | | | | | |
| | | | | | | | | | | | | | | | | |
| L1,92-111 | 920305 | D | | 1 | | | | | | | | | | | | |
| L1,92-023 | 921201 | S | | | | | | | | | 1 | | 1 | | | |
| | | | | | | | | | | | | | | | | |
| B3,A93-021 | 930418 | D | | 1 | | | | | | | | | | | | |
| B3,A93-055 | 930522 | S | | | | | | | | | | | 1 | | 1 | |
| P7,B93-050 | 930913 | S | | 1 | | | | | | | | | | | | |
| P3,A93-087 | 931009 | D | | | | | 1 | | | | | | | | | |
| D4,A93-087 | 931027 | S | | | 1 | | | | | | | | | | | |
| B1,A93-143 | 931207 | D | | | | | | | | 1 | | | | | | 1 |
| | | | | | | | | | | | | | | | | |
| L1,94-101 | 940111 | S | | | | | | | | | | | | | | 1 |
| | | | | | | | | | | | | | | | | |
| TOTAL | | | 41 | 17 | 8 | 7 | 15 | 6 | 5 | 17 | 17 | 8 | 3 | 3 | 13 | 13 |
| Percentage | | | 23.70% | 9.83% | 4.62% | 4.05% | 8.67% | 3.47% | 2.89% | 9.83% | 9.83% | 4.62% | 1.73% | 1.73% | 7.51% | 7.51% |

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Spec-ified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Periph-eral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| B1,A84-083 | 840920 | S | | | | | | | | 1 | | | | | | |
| B1,A87-047 | 870617 | D | | | | | 1 | | | | | | | | | |
| B1,A89-025 | 890309 | D | | | | | 1 | | | | | | | | | |
| B1,A93-143 | 931207 | D | | | | | | | | 1 | | | | | | 1 |
| B2,A84-092 | 841015 | D | | | | | 1 | | | | | | | | | |
| B2,A85-006 | 850111 | S | | | | | 1 | | | | | | | | | |
| B2,A87-079 | 871010 | D | | 1 | | | | | | | | | | | | |
| B2,A89-053 | 890419 | S | | | | | | | | | | 1 | | | | |
| B3,A84-030 | 840323 | S | | | | | | | | | 1 | | | | | |
| B3,A84-031 | 840324 | S | | 1 | | | | | | | | | | | | |
| B3,A85-064 | 850518 | S | | | | | 1 | | | | | | | | | |
| B3,A88-009 | 880128 | S | | | | | | | | 1 | | | | | | |
| B3,A93-021 | 930418 | D | | 1 | | | | | | | | | | | | |
| B3,A93-055 | 930522 | S | | | | | | | | | | | 1 | | 1 | |
| B4,A82-046 | 820510 | S | | | | 1 | | | | | | | | | | |
| B4,A82-067 | 820604 | S | | 1 | | | | | | | | | | | | |
| B4,A85-108 | 850823 | S | | | | | | | | 1 | | | | | | 1 |
| B4,A87-051 | 870624 | S | | 1 | | | | | | | | | | | | |
| B4,A88-090 | 880815 | S | | 1 | | | | | | | | | | | | |
| B4,A89-033 | 890327 | S | | | | | | | | | 1 | | | | | |
| B4,A90-099 | 900912 | D | | | | | | | | 1 | | | | | | |
| | | | | | | | | | | | | | | | | |
| B6,B90-007 | 900206 | S | | | | | | | | | | | | | | 1 |
| B7,B86-011 | 860203 | S | | | | | | | | | | | | | 1 | |
| B7,B86-034 | 860401 | S | | | | | | | | | 1 | | | | | |
| B7,B86-048 | 860602 | S | | | | | | | | | | | | | 1 | |
| B8,B86-074 | 861105 | S | | | 1 | | | | | | | | | | | |
| B8,B91-028 | 910315 | S | | | | | | | | | 1 | | | | | |
| | | | | | | | | | | | | | | | | |
| D2,90-024 | 900523 | S | | | | | 1 | | | | | | | | | |
| D2,A89-042 | 891217 | D | | 1 | | | | | | | | | | | | |
| D2,A90-008 | 900214 | D | 1 | | | | | | | | | | | | | |
| D4,A93-087 | 931027 | S | | | 1 | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| G2,82-814 | 821115 | S | | | 1 | | | | | | | | | | | 1 |
| G2,83-016 | 831202 | S | | | | | | | | | | | | | | 1 |
| G2,83-510 | 830215 | S | 1 | | | | | | | | | | | | 2 | |
| G2,83-606 | 830601 | S | | | | | | | | | 1 | | | | | |
| G2,83-707 | 830913 | S | 1 | | | | | | 1 | | | | | | | 1 |
| G2,83-814 | 831016 | S | | | | | | | | 1 | | | | | | |
| G2,83-815 | 831021 | S | | | | | | | | | | | | | | 1 |

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Specified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Peripheral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| G2,83-817 | 831102 | S | | | | | | | 1 | | | | | | | |
| G2,84-501 | 840115 | S | | | | | | | | | | | | | | 1 |
| G2,84-615 | 840427 | S | 2 | | | | | | | | | | | | | |
| G2,84-709 | 840731 | S | | | | | | | | 1 | | | | | | |
| G2,84-809 | 841017 | S | 1 | | | | | | | | | | | | | |
| G2,84-810 | 841202 | S | | | | | 1 | | | | | | | | | |
| G2,84-811 | 841205 | S | | | | | | | | | | | | 1 | | |
| G2,85-504 | 851117 | S | | | | | | | | 1 | | | | | 1 | |
| G2,85-612 | 850413 | S | | | | | | | | | | | 1 | | | |
| G2,85-613 | 850524 | S | | | | | | | | | | | | 1 | | |
| G2,85-708 | 850910 | S | | | | | | | | 2 | | | | | | |
| G2,85-816 | 851230 | S | | | | | | 1 | | 1 | 1 | | | | 1 | |
| G2,86-506 | 860311 | S | | | | | 1 | | | | | | | | | |
| G2,91-122 | 910711 | S | | 1 | | | | | | 1 | | | | | | |
| G2,91-13 | 910405 | D | | | 1 | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| L1,82-040 | 821102 | S | | | | | 1 | | | | | | | | | |
| L1,82-820 | 821101 | S | | | | | | | | | | | | | 1 | 1 |
| L1,83-002 | 830104 | S | 1 | | | | | | | | | | | | | |
| L1,83-009 | 830228 | S | | | | | | 1 | | | | | | | | |
| L1,83-534 | 830301 | S | 1 | | | | | | | | | | | | | |
| L1,83-535 | 830301 | S | 1 | | | | | | | | | | | | | |
| L1,83-605 | 830628 | S | | | | | | 1 | | | | | | | | |
| L1,83-641 | 830401 | S | | | 1 | | | | | | | | | | | |
| L1,83-728 | 830701 | S | | 1 | | 1 | | 2 | | | | | | | | |
| L1,83-828 | 831030 | S | 1 | | | | | | | | | | | | | |
| L1,83-829 | 831015 | S | | | | | | 1 | | | 1 | | | | | |
| L1,84-605 | 840522 | S | | | | | 1 | | | | | | | | | |
| L1,84-611 | 840513 | S | | | | | | | | | | 1 | | | | |
| L1,84-627 | 840515 | S | 1 | | | | | | | | | | | | | |
| L1,84-628 | 840515 | S | 1 | | | | | | | | | | | | | |
| L1,84-804 | 841022 | S | | | | | | | | | | | | | | 1 |
| L1,84-824 | 841101 | S | 1 | | | | | | | | | | | | | |
| L1,85-603 | 850513 | S | | 1 | | | | | | | | | | | | |
| L1,85-604 | 850628 | S | | | | | | | | | | 1 | | | | |
| L1,85-605 | 850515 | S | | | | | | | | | | | | | 1 | |
| L1,85-606 | 850615 | S | | | 1 | | | | 1 | | | | | | | |
| L1,85-631 | 850501 | S | 1 | | | | | | | | 2 | | | | | |
| L1,85-725 | 850801 | S | 1 | | | | | | | | | | | | | |
| L1,85-821 | 851115 | S | | | | | | | | | 1 | 1 | | | | |
| L1,86-503 | 860329 | S | | | | | | | | | | 1 | | | | |

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Spec-ified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Periph-eral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| L1,86-532 | 860301 | S | | | | 2 | | | | | 2 | 1 | | | | |
| L1,86-603 | 860605 | S | | | | | | | | | | | | | | 1 |
| L1,86-633 | 860601 | S | 1 | | | | | | | | | | | | | |
| L1,86-705 | 860730 | S | | | | | | | | 1 | | | | | | |
| L1,86-829 | 861101 | S | | | | | | | | | 1 | | | | | |
| L1,87-009 | 871007 | S | | 1 | | | | | | | | | | | | |
| L1,88-110 | 880417 | S | | | | | | | | 1 | | | | | | |
| L1,92-023 | 921201 | S | | | | | | | | | 1 | | 1 | | | |
| L1,92-111 | 920305 | D | | 1 | | | | | | | | | | | | |
| L1,94-101 | 940111 | S | | | | | | | | | | | | | | 1 |
| | | | | | | | | | | | | | | | | |
| P1,A82-134 | 821010 | S | | | | | | | | | | | | | 1 | |
| P1,A83-120 | 831016 | S | | 1 | | | | | | | | | | | | |
| P1,A83-123 | 831018 | S | | | | | 1 | | | | | | | | | |
| P1,A83-134 | 831027 | S | | | 1 | | | | | | | | | | | |
| P1,A83-149 | 831216 | D | 1 | | | | | | | | | | | | | |
| P1,A84-001 | 840105 | D | 1 | | | | | | | | | | | | | |
| P1,A84-019 | 840301 | D | 1 | | | | | | | | | | | | | |
| P1,A84-026 | 840314 | D | 1 | | | | | | | | | | | | | |
| P1,A86-141 | 860923 | S | 1 | | | | | | | | | | | | | |
| P1,A87-222 | 871115 | S | 1 | | | | | | | | | | | | | |
| P1,A88-045 | 880228 | D | 1 | | | | | | | | | | | | | |
| P1,A91-033 | 910302 | D | 1 | | | | | | | | | | | | | |
| P18,B87-113 | 870825 | D | 1 | 1 | | | | | | | | | | | | |
| P2,A83-133 | 831029 | D | 1 | | | | | | | | | | | | | |
| P2,A84-002 | 840118 | D | 1 | | | | | | | | | | | | | |
| P3,A82-025 | 820305 | S | 1 | | | | | | | | | | | | | |
| P3,A82-128 | 821005 | S | | 1 | | | | | | | | | | | | |
| P3,A83-105 | 830925 | D | | | | | | | | 1 | | | | | | |
| P3,A83-158 | 830912 | S | | | | | | | | | | | | | | 1 |
| P3,A85-110 | 851101 | S | | | | | | | | 1 | | | | | | |
| P3,A86-105 | 860704 | D | | | | | | | | | | 1 | | | | |
| P3,A87-083 | 870525 | D | | | | | | | | | | | | 1 | | |
| P3,A87-084 | 870525 | D | 1 | | | | | | | | | | | | | |
| P3,A87-179 | 870829 | D | 1 | | | | | | | | | | | | | |
| P3,A87-184 | 870901 | S | 1 | | | | | | | | | | | | | |
| P3,A87-210 | 871025 | S | | | | | | | | 1 | | | | | | |
| P3,A87-236 | 871202 | S | | | | | | | 1 | | | | | | | |
| P3,A89-096 | 890707 | D | | | | 1 | | | | | | | | | | |
| P3,A89-105 | 890806 | D | 1 | | | | | | | | | | | | | |
| P3,A89-140 | 891002 | D | | | | | | | | | | 1 | | | 1 | |

| | | | Fault Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SER Code | Date | Single/ Double | Not Spec-ified | Operator or Process Error | DCC PSU Failure | Sensor Failure | Other Plant | DCC Memory Parity | DCC Memory Other | DCC Periph-eral | DCC I/O Sensor System | DCC Fuse | DCC Bad Solder Joint | DCC Loose Conn'n | DCC Other H/W | DCC S/W |
| P3,A93-087 | 931009 | D | | | | | 1 | | | | | | | | | |
| P4,A83-012 | 830210 | S | 1 | | | | | | | | | | | | | |
| P4,A83-072 | 830825 | D | 1 | | | | | | | | | | | | | |
| P4,A83-138 | 831113 | S | 1 | | | | | | | | | | | | | |
| P4,A83-144 | 831116 | S | 1 | | | | | | | | | | | | | |
| P4,A83-999 | 831114 | S | 1 | | | | | | | | | | | | | |
| P4,A84-131 | 841112 | S | | | | | 1 | | | | | | | | | |
| P4,A85-079 | 850310 | S | | | | 1 | | | | | | | | | | |
| P4,A87-009 | 870119 | S | | | | | | | | | | | | | 1 | |
| P4,A87-011 | 870120 | S | | | | | 1 | | | | | | | | | |
| P4,A87-229 | 871119 | S | | | | | | | | | | | | | 1 | |
| P4,A88-122 | 880707 | S | | | 1 | | | | | | 1 | | | | | |
| P5,B82-163 | 821121 | S | | | | | 1 | | | | | | | | | |
| P5,B82-177 | 821202 | S | 1 | | | | | | | | | | | | | |
| P5,B84-036 | 840216 | S | 1 | | | | | | | | | | | | | |
| P5,B87-112 | 870825 | D | | | | | | | 1 | | | | | | | |
| P5,B89-080 | 890728 | S | | 1 | | | | | | | | | | | | |
| P6,B90-163 | 900914 | S | | | | 1 | | | | | | | | | | |
| P7,B91-091 | 910827 | S | | | | | | | | | 1 | | | | | |
| P7,B93-050 | 930913 | S | | 1 | | | | | | | | | | | | |
| P8,B86-175 | 860825 | S | 1 | | | | | | | | | | | | | |
| P8,B91-079 | 910621 | S | | | | | | | | | 1 | | | | | |
| P8,B91-088 | 910804 | S | 1 | | | | | | | | | | | | | |

APPENDIX D

# MULTI-ECHELON PROCESS PROTECTION

## D.1 Multi-echelon Protection Layers

Figure D-1 illustrates the typical layers of protection provided for modern plants which process hazardous materials. This multi-echelon protection layer approach to safety is also used in nuclear-power generating stations. Each layer of protection consists of a grouping of equipment and/or administrative controls, that function in concert with other layers to control process risk. These protection layers are described below, in the order of activation during an escalating accident.

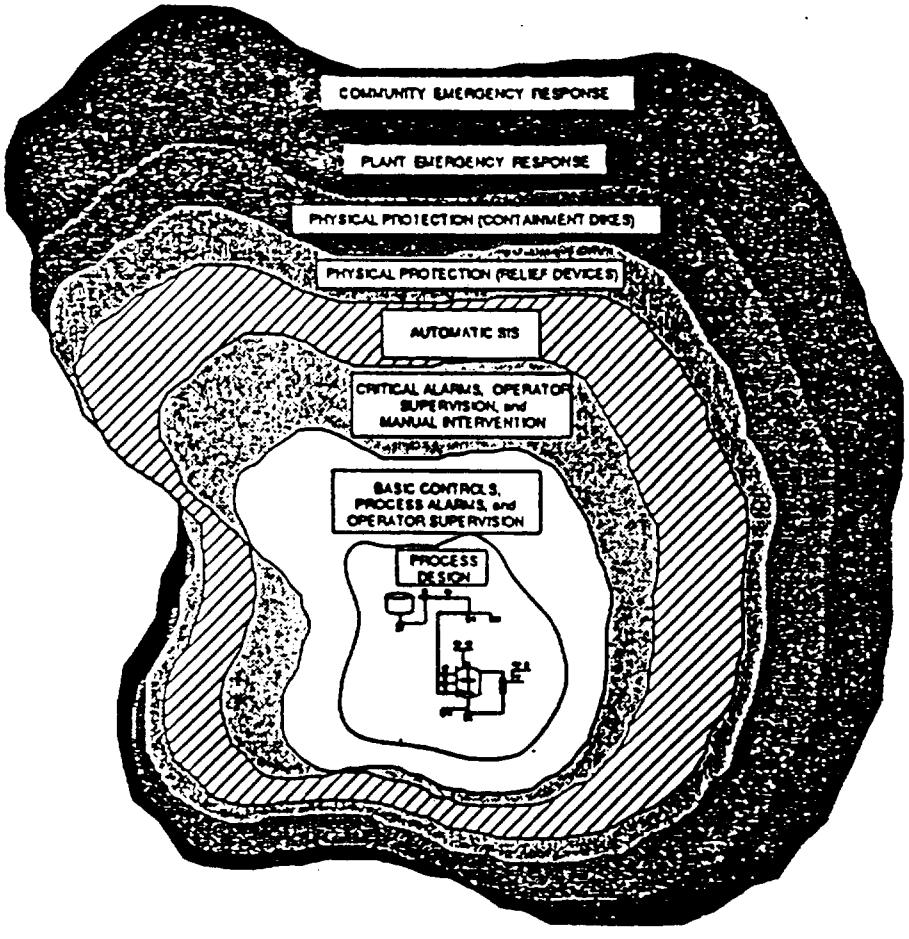


Figure D-1. Multi-echelon Protection Layers

1. Risk reduction begins with the most fundamental elements of the process design (e.g., process selection, selection of site, plant layout, application of inherently safe design practices, etc.). This type of protection is passive, in that it mitigates potential hazards by virtue of design decisions and it represents the first level of protection.

2. Next comes the basic process control system (BPCS), supplemented by operator supervision, with a further layer provided by the alarm system and operator-initiated corrective actions. These layers would be represented by the RRS within the CANDU nuclear generating stations.

3. The next layer, known as the safety interlock system (SIS), is used to take corrective action when failures occur in the process and BPCS layers. This type of protection is active, in that it initiates a specific action when a hazardous event is likely. This layer would be represented by shutdown systems 1 and 2.

4. The next layer is in the form of physical protection, such as venting devices, to prevent equipment failure from over-pressure.

5. If all of the lower levels of protection fail to function and a release occurs, dikes may be used to contain such things as liquid spills. This layer would be represented by the containment system.

6. Finally, emergency response plans at the plant and community level provide the outermost levels of protection. Most failures in well-designed and well-operated processing plants are contained by the first one or two protection layers. The middle levels guard against major releases and the outermost layers provide mitigation response to very unlikely major events.

## D.2 Independent Protection Layers

A protection layer is a distinct part of the process and plant design that is intended to avoid the occurrence, or to reduce the effect, of a specific hazardous event. When significant hazards cannot be avoided by inherently safe process and process equipment selection, instrumented protective functions assume greater importance. Assurance becomes necessary that these protection layers function so that a failure of one of the inner layers does not disrupt the effectiveness of an outer, backup layer.

Independent Protection Layer (IPL) is the term used to indicate protective systems that are designed to prevent, or to mitigate, identified events and that meet tests of specificity, independence, dependability, and auditability. Specificity describes a situation in which the IPL is designed solely to prevent, or to mitigate, the consequences of one potentially hazardous event. The BPCS often functions as a protective layer, however, its task is multipurpose. As such it fails the test of specificity, as its first purpose is to regulate the process. Therefore, the BPCS (and in this case, the RRS) is not considered to be an IPL.