NRC Research and/or Technical Assistance Rept

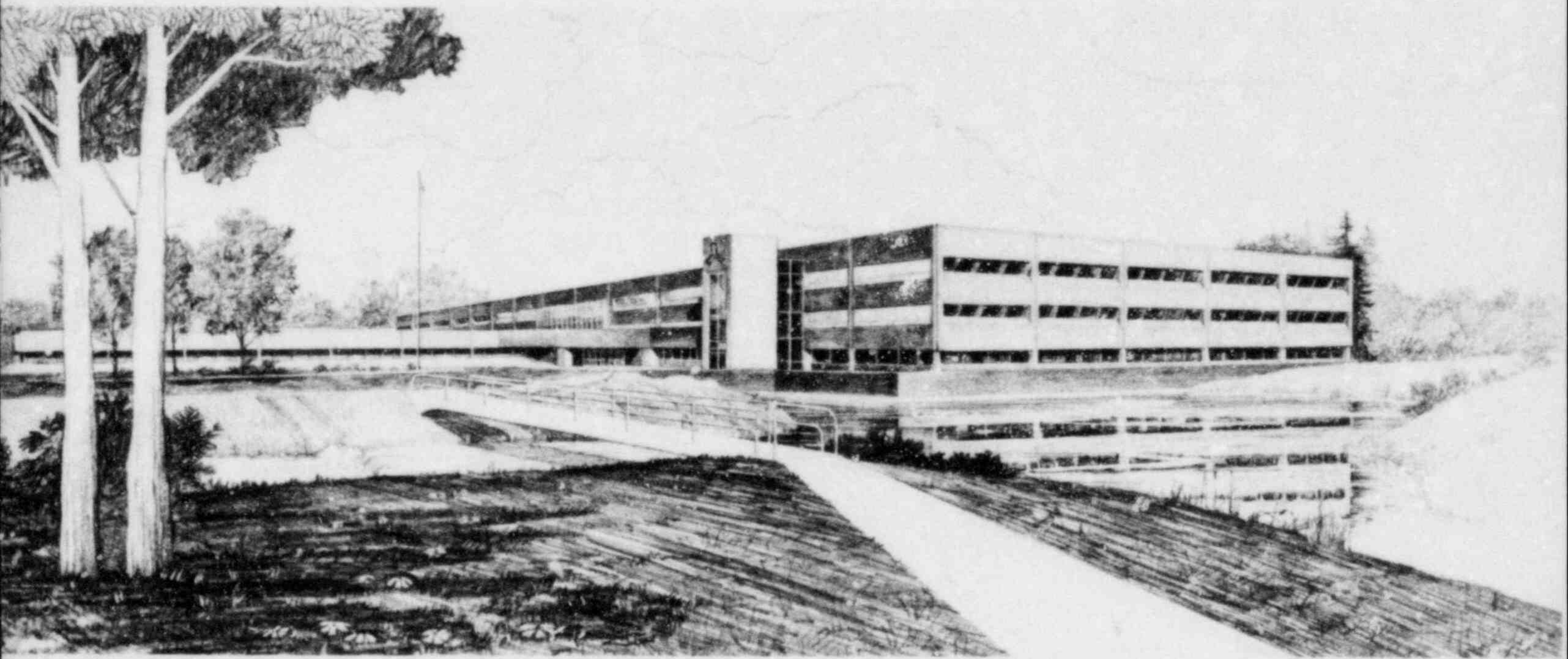
PDR

EGG-EE-6052
September 1982

SIGNAL ISOLATION DEVICE AND STORED PROGRAM DIGITAL COMPUTER PROBLEMS EXPERIENCED BY U. S. COMMERCIAL NUCLEAR POWER PLANTS

R. R. Rohrdanz

Idaho National Engineering Laboratory
Operated by the U.S. Department of Energy



This is an informal report intended for use as a preliminary or working document

Prepared for the
U.S. NUCLEAR REGULATORY COMMISSION
Under DOE Contract No. DE-AC07-76ID01570
FIN No. A6370

EG&G Idaho

EG&G Idaho, Inc

FORM EG&G-398
(Rev. 03-82)

INTERIM REPORT

Accession No. ____________

Report No. EGG-EE-6052

Contract Program or Project Title:

Research to Assess Microprocessor-Based System Design and
Associated Isolation Devices

Subject of this Document:

Signal Isolation Device and Stored Program Digital Computer Problems
Experienced by U. S. Commercial Nuclear Power Plants

Type of Document:

Informal Report

Author(s):

R. R. Rohrdanz

Date of Document:

September 28, 1982

Responsible NRC Individual and NRC Office or Division:

D. W. Boehm, Office of Nuclear Regulatory Research (RES)

> This document was prepared primarily for preliminary or internal use. It has not received full review and approval. Since there may be substantive changes, this document should not be considered final.

EG&G Idaho, Inc.
Idaho Falls, Idaho 83415

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C.
Under DOE Contract No. DE-AC07-76ID01570
NRC FIN No. A6370

INTERIM REPORT

INTERIM REPORT

SIGNAL ISOLATION DEVICE AND STORED PROGRAM DIGITAL COMPUTER PROBLEMS EXPERIENCED BY U.S. COMMERCIAL NUCLEAR POWER PLANTS

R. R. Rohrdanz

Published September 1982

EG&G IDAHO, INC.
Idaho Falls, Idaho 83415

Prepared for the
U.S. NUCLEAR REGULATORY COMMISSION
Washington D. C., 20555
Under DOE Contract No. DE-AC07-76ID01570
FIN No. A6370

ABSTRACT

This interim report identifies problems with Signal Isolation Devices and Stored Program Digital Computers as experienced by U.S. Commercial Nuclear Power Plants. The information was gathered from Licensee Event Reports (LERs) which were prepared by the power plants involved.

These problems occurred from January 1976 to June 1982. This report identifies the methodology used to screen LERs, presents applicable LER summaries, evaluates the problems associated with the subject isolators and computers, and recommends corrective actions to minimize future problems.

FIN No. A6370

SUMMARY

Based upon Licensee Event Reports (LERs), signal isolation devices used in Commercial Nuclear Power Plants have not had unacceptable types or numbers of failures. However, the fact that there were LERs related to signal isolators indicates some attention should be directed to these devices. This attention should be directed towards achieving better reliability. Better component selection, possibly by specifying screened burned-in components, should be implemented as a means to improve reliability. Reliability can also be improved by attention to design, fabrication, installation, and maintenance and each of these should be addressed when appropriate.

In contrast to the signal isolator problems, the problems from all causes associated with computers are much more serious. The computer problems associated with plants other than Arkansas Nuclear 2 (AN 2) may be within an acceptable norm. However the computer problems experienced at AN 2 seem excessive. Microcomputers similar to those at AN 2 typically have hardware failure rates on the order of one in ten thousand hours. It would appear that the failure rate for AN 2 is much higher (more failures) than would reasonably be expected from microcomputer hardware.

The numbers, severity, and consequences of the PPS problems experienced by AN 2 during startup and early operation should be compared with those of at least several similar plants which have hardwired PPSs. Calvert Cliffs 2 might be one to include, since it is about the same size, is also a Combustion Engineering plant, and used the same engineer and constructor (Bechtel). It preceeded AN 2 in design, construction, startup, and operation by two to three years. Arkansas Nuclear 1 might not be a good plant to include in the comparison, since the reactor was supplied by Babcock and Wilcox, and the PPS may have significant differences. If the problems of AN 2 and the group of similar plants are comparable, then failure analysis and corrective action may adequately address the PPS problems at AN 2. If the AN 2 problems are significantly more extensive in

number, severity, or consequence, a review of the design and licensing process for the PPS computer system at both AN 2 and future plants should be conducted.

Computer system designs in general should be improved by the use of screened or burned-in components, extensive component and system testing, improved diagnostic hardware and software, incorporation of error or fault detection features with automatic switchover to spare circuits or by the use of fault tolerant features. If possible, diversity of both hardware and software should be used in future applications. However, diversity should be judiciously used, since as diversity increases, so may the maintenance effort.

CONTENTS

TABLES

ACRONYMS

AN 2	Arkansas Nuclear 2
CE	Combustion Engineering
CEA	Control Element Assembly (Control Rod Assembly)
CEAC	Control Element Assembly Calculator
CPC	Core Protection Calculator
CPU	Central Processing Unit
DNBR	Departure From Nucleate Boiling Ratio
GE	General Electric
LER	Licensee Event Report
PPS	Plant Protection System

DEFINITION OF TERMS

The numbers in brackets [] refer to the IEEE Standards in which these definitions are used.

1. Analog Signal--An information signal where the signal variable ranges continuously between a low value and a high value. For example a voltage that can continuously range between 0 and 10 volts.

2. Class 1E--The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment [308, 334, 344, 383, 384, 494].

3. Bit--A binary value (0 or 1) used to represent numbers, characters, or system states in a computer.

4. Computer--As used in the text, computer refers to a stored program digital computer.

5. Control System--The control system consists of all instrumentation and control equipment not included in the scram or engineered safety features systems, including automatic and manual process controls, presentations of information to the operator (plant monitoring system), and plant computer(s) that are not part of scram or ESF actuation systems.

6. CPU--Central Processing Unit, consists of the registers and logic required to perform the basic logical and arithmetic operations which constitute a program.

7. Digital Signal--An information signal where the signal consists of a collection of one or more bi-level signals or bits. The information content is related to the presence or absence of these bits and the relative importance of ea-h of the bits.

8. Fault Tolerant--A fault tolerant computing system has the built-in capability (without external assistance) to preserve the continued correct execution of its programs and input/output (I/O) functions in the presence of a certain set of operational faults.

9. Isolation--Isolation is defined as the electrical and information (signal) separation between redundant systems, the trip system, the control system, and the engineered safety system to assure independence and integrity of function.

10. Isolation Device--A device in a circuit which prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits [384].

11. Isolation Impedance--The internal impedance presented by an isolation device between its input side and its output side.

12. Non-Class 1E System--Equipment or systems which do not have the Class 1E safety classification.

13. Redundancy--A redundant system is defined as a system that duplicates the essential function of another system to the extent that either may perform the required function regardless of the state of operation or failure of the other system.

14. Reliability--The characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.

15. Safety-Related--As applied to electrical equipment and systems; these are those equipments and systems that are relied upon to remain functional during and following design-basis events to assure

    1. The integrity of the reactor coolant pressure boundary

    2. The capability to shut down the reactor and maintain it in a safe shutdown condition

    3. The capability to prevent or mitigate the consequences of accidents which could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines.

16. Plant Protection System (PPS)--The plant protection system consists of sensors, signal processors, logic, and actuation initiation devices necessary to effect reactor trip or scram, including essential auxiliary systems. The plant protection system is also known as the reactor trip system (RTS).

17. Security--Security includes those design practices and administrative procedures/controls to ensure that the availability of the computer system is not jeopardized through malevolent, unintentional, or unauthorized access/perturbation.

18. Stored Program Digital Computer--A computer that executes programmed instructions from a stored medium as opposed to dedicated logic (function is fixed at the design stage using combinational and sequential circuits) and analog (linear) circuits.

SIGNAL ISOLATION DEVICE AND STORED PROGRAM DIGITAL COMPUTER PROBLEMS EXPERIENCED BY U.S. COMMERCIAL NUCLEAR POWER PLANTS

1. INTRODUCTION

The NRC has concerns related to the application of signal isolation devices used in safety related systems in U.S. commercial nuclear power plants. This report has been prepared at the request of the NRC to present a listing of Licensee Fvent Reports (LERs) which relate to operational experience of signal isolation devices.

In searching for signal isolator LERs it was observed that there were many more LERs which address problems with Stored Program Digital Computers (computers). EG&G Idaho, Inc. has a task to assess the design issues related to the use of computers for safety and control systems,[6] so LERs dealing with computers have been included in this report. The information related to the operation of computers at plants will assist continued effort on this task.

Signal isolation devices are of dual interest because their isolation provides separation and independence in safety systems and because they are often used when instrumentation and control signals are transferred to, from, or between computers in nuclear power plants.

Signal isolation devices are quite common but the number of computers presently in use is quite limited. However, the number of each will increase significantly in the future, both as new nuclear power plants become operational and as existing nuclear power plants, particularly older plants, are retrofitted to upgrade safety systems and to improve plant operational efficiency.

This report identifies problems existing nuclear power plants have had with signal isolation devices and computers. The problems identified are associated with both Safety Related (Class 1E) and Non-Safety Related (Non-Class 1E) equipment. The evaluation of the problems identified will be used in work on signal isolation devices and the application of computers in nuclear power plants performed by EG&G Idaho, Inc.

The easiest method of obtaining information pertaining to signal isolator and computer problems experienced by Commercial Nuclear Power Plants is from Licensee Event Reports (LERs). LERs are required by the NRC for reporting of unusual occurrences in Commercial Nuclear Power Plants. LERs do have limitations (discussed in Section 2, Methodology), however they do identify important problems encountered by nuclear power plants. Due to these limitations some problems may be overlooked or will be incorrectly described, but if taken as trend data the information gained will be both typical and useful, giving a good cross section of serious problems.

LERs from January 1976 through June 1982 were screened to provide the information in this report. No plants or vendors were contacted for supplemental information so the information is limited to what is extracted or inferred from LERs. The applicable LERs are summarized in this report and conclusions are drawn regarding problems associated with isolators and computers.

2. METHODOLOGY

The information obtained for this report was obtained from LERs. The report is therefore subject to the limitations of the LER reporting system. LERs are prepared whenever a Commercial Nuclear Power Plant has a reportable occurrence. These occurrences or events are as defined in 10 CFR 50.72 and in the Technical Specification for the involved plant. LERs are abstracts, prepared in accordance with NUREG-0161.[5] The report format is standardized to insure that necessary basic information is included. The description of the problem is limited to permit the LER to be a one page document. Additional information by supplemental letter is required, but this information is not available when searching LERs. To facilitate searching, the problems are categorized on the LER by system, component, and cause. This greatly assists in reviewing LERs since many can be quickly identified as not related to the subject of interest. Those which remain can then be examined in more detail.

The ability to screen LERs quickly and select only those of potential interest is very important since approximately 21,000 have been prepared from January 1976 to date. Even when selecting only those LERs which are categorized as involving an I&C component, there are about 6,000. The categorization process speeds the search, but also introduces the possibility of overlooking events which were not categorized with the same headings used in the search. This arises because the LER originator may not fully understand the cause, and thus selects an incorrect cataloging code. The originator may also use terminology that is different than used by the searcher or by other LER originators. An example of this might be the failure of an isolation amplifier in a transmitter where the isolation amplifier is a component in the transmitter. The LER may clearly identify that the isolation amplifier failed, or may only indicate that the transmitter failed. In the latter situation, a search for failed isolation amplifiers would not select the LER because the failed isolation amplifier was not mentioned.

LERs must be submitted in a timely manner, depending on the type, usually 10 days (or 2 weeks) or 30 days. On many occasions, the cause or other details of the event are not fully understood before the LER is submitted. A revised LER is normally required when followup details are needed, but this may not be prepared, or may be overlooked in a search.

Categorizing (coding) component, systems, causes, etc., on the LER permits the LERs to be selected or screened by codes or categories with relative ease by computer when the LERs are in an appropriate data base. A data base has been established, and the search performed for this report took advantage of screened LERs. NUREG/CR-1740 EGG-EA-5388[1] is one example.

The LER information dissimination system has recently been improved in that the LERs gathered by the NRC are published in NUREG/CR-2000 [2,3,4] which is issued monthly. These documents provide category cross references to ease the search effort.

In summary, the information gathered was based on LERs; no vendors or plants were contacted. Because of the nature of the LER system and the search and screening effort to locate LERs of interest, the information gathered lacks detail but does document the basic types and numbers of problems.

3. EXCERPTS OF SIGNAL ISOLATION DEVICE LERS

The following problem descriptions are excerpts of LERs which address signal isolation device problems experienced by U.S. Commercial Nuclear Power Plants.

3.1 Calvert Cliffs 1 and 2

From June 1979 to October 1980, problems with Transmation Inc. Isolating Transmitters (Model No. 2301 T) were identified. These are isolation devices which pass signals to the RPS and ESFAS. The problems resulted in unsafe (nonconsertive direction) failures of setpoints.

The faulty isolators were not able to be calibrated and were returned to the manufacturer. The manufacturer replaced several industrial grade capacitors with Mil Spec capacitors to improve the reliability of the devices. Field changes[12] for the remaining units were planned and should have been completed by January 1, 1981.

The dates of these LERs were:

Unit 1	September 1979[7]
Unit 2	June 1979[8]
Unit 2	March 1980[9]
Unit 2	September 1980[10]
Unit 2	October 1980[11]

No subsequent problems have been identified.

In February 1982 at Calvert Cliffs 2 an Isolator Module, Vitro Lab Model No. 1628-1070 failed in the conservative direction.[13] This resulted in the application of a trip signal to the activation channel. The isolator was replaced. No subsequent failures have been found.

3.2 Cooper

In August 1977 a defective isolation amplifier was found.[14] This was a component in a General Electric Model 136B 3088AAG1 Summer Unit. The isolation amplifier was intermittent and caused an Average Power Range Monitor (APRM) upscale alarm. The amplifier was replaced. This was a conservative direction failure. No other LERs dealing with these devices have been found.

3.3 Beaver Valley 1

In November 1980 an isolation amplifier was found to exhibit drift.[15] The amplifier was repaired. It was a Westinghouse supplied component. No other LERs dealing with these devices have been found.

3.4 Arkansas Nuclear 2[a]

In August 1979 a Core Element Assembly Calculator (CEAC) #1 optical isolator failure resulted in a dropped "bit" which caused a CPC channel trip.[16] This was a failure in the conservative direction. The data link was repaired within one hour.

In October 1980 the CEAC #2 experienced three optica, isolator failures.[17] The bit 12 isolator failed and was replaced. There had been five previous similar failures.[18]

[a] See Appendix A for a system description.

4. EXCERPTS OF STORED PROGRAM DIGITAL COMPUTER LERS

The following problem descriptions are excerpts of LERs which address Stored Program Digital Computer problems experienced by U.S. Commercial Nuclear Power Plants.

4.1 Calvert Cliffs 1

On December 9, 1981, a plant computer failure occurred.[19] A memory track failed on the rapid access disk, which is part of the plant computer. A spare track was selected, the program reloaded, and the computer operation checked. The computer was out of service for 2 hours 15 minutes.

On December 15, 1981, a plant computer failure occurred.[20] This failure was caused by a failure of a typewriter drive system during entry of program instructions. The computer recognized the problem. The typewriter was replaced with a spare, the program reloaded, and the system returned to operation within three hours.

4.2 Hatch 1

In January 1982 a process computer problem occurred.[21] The nuclear correlation coefficients used in the process computer were miscalculated due to an error in the General Electric (GE) generation code. The error was very small and conservative. Corrections were to have been made prior to startup. GE instigated an action plan to prevent a future recurrence.

4.3 St. Lucie 1

In December 1981 a computer software error was discovered.[22] While performing post refueling outage power ascension physics tests, more than three in core detector alarms were in the alarm condition. Response action to these alarms was not taken for eight hours, apparently because the precision of the setpoints was under investigation. The alarms were caused by errors in the vendor-supplied computer software which contained incorrect flux inputs in arriving at the alarm setpoints. Correct setpoints were entered into the system within six hours. Both the vendor personnel and operators have taken corrective measures.

4.4 Farley 2

In February 1982 a computer communication link failure occurred causing the stack effluent monitor to be inaccurate.[23] The event was caused by dirty contacts and a faulty communication link between a radiation monitor and the computer processing radiation data. The contacts were cleaned, the communication link repaired, and radiation monitor declared operable.

4.5 McGuire 1

In April 1982 a computer problem occurred.[24] An operator in training, while attempting to address the status of a fire zone through the Honeywell Fire Detection System (computer), mistakenly dumped the CPU memory, which resulted in the fire detection system being declared inoperable. Access to the CPU memory is administratively controlled. Additional training and administrative controls were to be initiated.

4.6 Arkansas Nuclear 2--Control Element Assembly Calculator (CEAC)[a]

On July 21, 1980 CEAC #1 failed.[25] Investigation did not reveal the cause for the failure. The system software was reloaded, a system periodic test performed with good results, and the system returned to operation.

On July 24, August 28 and October 8, 1980 CEAC #2 was found inoperable.[26] Investigations did not reveal the cause of the failures. In all cases the system was returned to normal operating status by reinitializing the system. The vendor, Combustion Engineering (CE), initiated an evaluation of the problems in an effort to solve them.

[a] See Appendix A for a system description.

In October 1980 four more failures of the CEAC #2 occurred. The first three were traced to an optical isolator for bit 12 (See Paragraph 3.4). The last failure was traced to a faulty OP module card.[27] The faulty card was replaced and the CEPC returned to normal operation.

On January 28, 1982 CEAC #1 indicated an erroneous indication for CEA #61.[28] This was traced to a High Level Mux Gate in CEAC #1. This was replaced and CEAC #1 was returned to service.

On April 1, 1982 CEAC #2 failed by momentarily indicating that one CEA was inserted farther than determined by other indications.[29] This problem existed only a short time. The CEAC was removed from service and computer diagnostics were initiated. No abnormality was revealed. Monthly surveillance was performed which indicated the CEAC was operable and it was then returned to service.

4.7 Arkansas Nuclear 2--Core Protection Calculator (CPC)[a]

On January 9, 1979 CPC "B" failed which produced three trip signals.[30] The occurrence was coincident with a panel ground alarm for that PPS channel. The trip signals cleared when the alarm was reset. Investigation revealed that the ground fault relays fell out on low bus voltage, which did not necessarily coincide with a ground fault. The CPC was returned to service. The investigation of the power loss was continued.

On January 27, 1979 CPC "B" failed, resulting in two trip signals.[31] Investigation revealed the analog high level amplifier card was not properly seated in its connector. The card was reseated. The CPC was functionally tested and returned to service. While troubleshooting this problem, cable connections in CEAC #1 were disturbed causing CEAC deviation alarms, which were reset following CPC "B" repair.

On January 28, 1979 both CPC "C" and "D" failed.[32] Both produced two trip signals in their respective PPS channels. The CPC "D" failure was

[a] See Appendix A for a system description.

caused by the channel DC power supply which had tripped. The power supply was replaced. The CPC "C" failure appeared to be non-repetitive and was unrelated to the CPC "D" failure. Both CPC channels were returned to operation.

In June 1979 CPC "A" gave two trip signals when the CPC was taken out of bypass.[33] All inputs were verified and a CPC functional test was successfully completed. No cause for the failure could be identified and the channel was returned to service.

On August 18, 1979 CPC "B" failed causing two trip signals.[34] The problem was caused by a failed memory module which was replaced. The CPC was returned to service.

On August 20, 1979 all (CEAC) inputs to all of the CPCs were placed in the INOP (inoperative) mode following spurious penalty factor signals which caused a reactor trip.[35] The high CEAC penalty factors were caused by dirty input card contacts. The card edge connector was cleaned and the system verified operational.

In September 1979 CPC "C" failed.[36] Investigation revealed a failed Reactor Coolant Pump "D" speed input. This was repaired and the channel successfully functionally tested and returned to service.

In December 1979 CPC "C" causing two trip-signals.[37] Investigation revealed a data link failure between the CPC and the CPC operator console. This was repaired, and the CPC was restarted and restored to operational status.

On December 21, 1979 an event similar to that described in Paragraph 4.7 (September 1979) occurred.[38] The CPC "C" failed due to a failed pump speed input. The speed indication returned to normal within 30 minutes. No cause of the failure could be determined. The speed probe and cable were replaced during the next outage to prevent recurrence.

On January 7, 1980 CPC "B" failed.[39] The exact cause could not be determined. (CE was developing software to aid in future diagnostics of CPC problems.)

On January 10, 1980 CPC "C" failed.[40] During "trouble shooting," the system restarted on its own when the Initialization button was pressed. Checks were performed which verified the CPC acceptable and it was returned to service. No cause for the failure could be found.

On January 23, 1980 CPC "B" failed.[41] The symptom was a display of "Analog Input Fail Function Code" which signifies an off normal input signal. The exact cause of the failure could not be determined. The CPC was restarted and declared operable within 1/2-hour.

On January 28, 1980 CPC "B" failed.[42] The cause could not be determined. The CPC was restarted, functionally tested, and returned to service within 1-1/2 hours.

On July 20, 1980 CPC "A" received three auto restarts within a 12 hour period.[43] Investigation did not reveal the exact cause, but high CPC room temperature was suspected. The room temperature was returned to normal, the CPC was functionally tested and returned to operable status.

On July 30, 1980 and on November 20, 1980 CPC "D" failed because the program halted.[44] The "watchdog" timer timed out preventing console communications, which rendered the CPC inoperable. Investigation did not reveal the root cause. The CPC system was reinitialized and returned to service.

In November 1980 CPC "A" failed because of a failure in the data link between the CPC and the CPC operator console.[45] A defective data link card was replaced and the CPC returned to operable status. This is similar to the problem which occurred on CPC "C" in December 1979.

In November 1981 it was discovered that appropriate (correct) DNBR Penalty Factors were not included in the CPC DNBR calculations.[46] As a result, it initially appeared that the reactor was operating outside the acceptable region described the Technical Specifications. Updated factors for appropriate calculations were entered in the CPCs. Later, it was determined that the change in factors had only a small effect on the power operating limit margin, and that the rector had not been operated outside the acceptable region (LER 81-044 Rev. 1). Administrative procedures have been initiated to ensure correct factors will be used in the future.

5. EVALUATION

It is evident in reviewing the LER excerpts more information is needed to fully understand each "event." For many LERs, the seriousness, cause of the problem, or the correction cannot be determined in enough detail to make firm or detailed recommendations. However, the fact that a LER was prepared indicates a problem existed. The information available in the LERs has been summarized in condensed form, and general trends can be observed. Although detail is lacking in many LERs, the trend information is still valid.

The LER excerpts presented in Sections 3 and 4 have been condensed and presented in Tables 1, 2, 3, and 4. The following evaluations are based on the information in the LER excerpts and tables.

5.1 Signal Isolation Devices

The LERs related to isolation devices described both analog and digital isolators.

5.1.1 Analog Signal Isolation Devices

Eight LERs addressed isolators from four different manufacturers. All failures involved hardware failure (in contrast to operator error or other causes). The Transmation Inc. isolator failures show the only trend for a single manufacturer, that of degraded commercial grade capacitors. The problems with commercial grade capacitors might have been avoided by more attention to design, failure analysis, and life testing including screening and burn-in. The manufacturers fix was replacement with Mil Spec capacitors which gives credence toward encouraging designs utilizing Mil Spec or screened and burned-in components.

The remaining failures, one each from three vendors seem random and no trend information is evident, except that all isolators were identified with problems where the output did not follow the input (i.e., drift,

TABLE 1. SUMMARY OF ISOLATOR LERS

Plant	Symptom	Cause	Correction	Frequency/Paragraph	Comments
Calvert Cliffs 1 & 2	Output drift	Degraded capacitors	Replace with Mil Spec capacitors	5 plus field change (Para. 3.1)	Transmation Inc.--Analog Isolator--hardware failure
Calvert Cliffs 2	Spurious trip signal	Unknown	Replace isolator	1 (Para. 3.1)	Vitro Lab--Analog Isolator --hardware failure
Cooper	Incorrect amplifier output	Unknown	Replace amplifier	1 (Para. 3.2)	General Electric--Analog Isolator--hardware failure
Beaver Valley 1	Output drift	Unknown	Repair isolator	1 (Para. 3.3)	Westinghouse--Analog Isolator--hardware failure
Arkansas Nuclear 2	Failed data link	Failed optical isolator	Replace isolators	9 (Para. 3.4 and 4.6)	Combustion Engr. (System Engineering Labs)--digital isolators--hardware failure

TABLE 2. SUMMARY OF COMPUTER LERS--OTHER THAN ARKANSAS NUCLEAR 2

Plant	Symptom	Cause	Correction	Frequency/Paragraph	Comments
Calvert Cliffs 1 (a)	Computer failure	Memory track failure	Switch to spare track	1 (Para. 4.1)	Hardware failure
Calvert Cliffs 1 (b)	Computer failure	Typewriter drive failure	Replace typewriter	1 (Para. 4.1)	Hardware failure
Hatch 1	Process computer problem	Code error	Correct code	1 (Para. 4.2)	General Electric supplied computer--software error
St. Lucie 1	In-core detector alarms	Incorrect alarm setpoints	Fix setpoints	1 (Para. 4.3)	Software error
Farley 2	Stack effluent monitor inaccurate	Computer communication link failure	Clean contacts and repair link	1 (Para. 4.4)	Hardware failure
McGuire 1	Fire detection system inoperative	Operator error dumped memory	Reload memory--train operator	1 (Para. 4.5)	Operator error

TABLE 3. SUMMARY OF COMPUTER LERS--ARKANSAS NUCLEAR 2--CEAC

Item	Symptom	Cause	Correction	Frequency/Paragraph	Comments
a	CEAC #1 inoperative (crashed)	Unknown	Reload system software/restart	1 (Para. 4.6)	None
b	CEAC #2 inoperative	Unknown	Reinitialize system	3 (Para. 4.6)	Combustion Engineering investigating problem
c	CEAC #2 failure	Faulty OP module card	Replace card	1 (Para. 4.6)	Hardware failure
d	CEAC #1 output error	High level mux gate failure	Replace gate	1 (Para. 4.6)	Hardware failure
e	Momentary CEAC #2 output error	Unknown	None, system returned to normal	1 (Para. 4.6)	None

TABLE 4. SUMMARY OF COMPUTER LERS--ARKANSAS NUCLEAR 2--CPC

Item	Symptom	Cause	Correction	Frequency/Paragraph	Comments
a	CPC B spurious trip	Panel ground alarm	Reset alarm	1 (Para. 4.7)	Investigation continuing--exact cause not understood
b	CPC B spurious trip	Analog high level amplifier card not seated	Seat card	1 (Para. 4.7)	Hardware failure
c	CPC D spurious trip	Tripped DC power supply	Replace power supply	1 (Para. 4.7)	Hardware failure
d	CPC C spurious trip (non-repetitive)	Unknown	None	1 (Para. 4.7)	Nonrepetitive failure
e	CPC A spurious trip when taken out of bypass	Unknown	Unknown	1 (Para. 4.7)	None
f	CPC B spurious trip	Failed memory module	Replace memory module	1 (Para. 4.7)	Hardware failure
g	Spurious penalty factor signals from CEACs to CPCs	Dirty input card contacts	Clean card edge connectors	1 (Para. 4.7)	Hardware failure
h	CPC C failure	Faulty external input signal	Repair external circuit	2 (Para. 4.7, September 1979 and December 1979)	External hardware failure

TABLE 4. (continued)

Item	Symptom	Cause	Correction	Frequency/Paragraph	Comments
i	CPC A and C spurious trips (different occasions)	CPC to CPC operator console data link failure	Repair data link	2 (Para. 4.7, December 1979 and November 1980)	Hardware failure
j	CPC B failure	Not determined	None	2 (Para. 4.7, January 7 and 28, 1980)	Combustion Engineering developing diagnostic software
k	CPC C failure	Unknown	None	1 (Para. 4.7)	System restarted when initialization button was pressed
l	CPC B failure--off normal input signal)	Unknown	None	1 (Para. 4.7)	None
m	CPC A received 3 auto restarts within 12 hours	Suspect high room temperature	Return room temperature to normal	3 (Para. 4.7)	None
n	CPC D program halt	Watch dog timer timed out	System reinitialized	1 (Para. 4.7)	Cause not understood
o	Incorrect plant operation suspected	Incorrect DNBR penalty factors used	Update factors	1 (all CPCs) (Para. 4.7)	Software constant error

spurious signal, etc.). There are no reports of an isolator failing in its function as an isolator, i.e., a failure on the output transferred to the input, etc. More attention to design and testing probably would have reduced the problems identified. The use of components specified for environment and lifetime should improve reliability.

5.1.2 Digital Signal Isolation Devices

Seven LERs addressing a total of nine failures of digital optical isolators. These were all at Arkansas Nuclear 2 and probably were from the same manufacturer. The failures were hardware failures, apparently the devices failed to pass a signal from input to output.

These failures all occurred early in the life of the equipment since the failures occurred while the plant was in startup and during the first six months of commercial operation (August 1979 to October 1980). Since no failures have been identified with these devices for the 18 months since the last LER (October 1980), these failures may have been due to infant mortality. More attention to selection of these devices and a burn-in program should minimize future, similar occurrences.

5.2 Stored Program Digital Computers

The LERs related to computers are more difficult to analyze than those of isolators. The LERs associated with plants other than Arkansas Nuclear 2 (AN 2) are reasonably definitive, providing far more information than those of AN 2. The AN 2 LERs may lack definition due to the complexity of the AN 2 computer systems. AN 2 is the first and presently the only U.S. commercial nuclear power plant to use computers in the Plant Protection System (PPS). AN 2 had many LERs which left events poorly defined and unresolved, i.e., the problem, cause and correction lacked an adequate description.

Collectively the computer LERs can be grouped by cause as follows:

10 LERs addressed	10 computer related hardware failures
2 LERs addressed	2 external (noncomputer) failures
2 LERs addressed	2 software program errors
1 LER addressed	1 software constant error
1 LER addressed	1 operator error
14 LERs addressed	16 problems of unknown cause and/or correction

The identified computer hardware problems (10) are far more common than the identified software problems (3) but the problems of unknown cause (16) are as common as all other problems combined. If only AN 2 problems are considered, the problems of unknown cause (16) exceed all others (10) significantly. The unknown cause problems probably fall into two classes, hardware or software failures. The number of each cannot be established from the LER review. The problems of unknown cause were usually associated with an undefined correction.

The problems associated with unknown cause and nebulous corrections at AN 2 may have been properly resolved, but the LERs do not give confidence that such follow-up occurred. If the problems described were associated with a different application of computers, they might be tolerable. When associated with a PPS, these problems indicate additional effort is needed. This effort should include a formal failure analysis program, a good reporting system and corrective actions when necessary. A comparison with similar plants having hardwired PPSs should be considered.

The problems described fall into categories one would associate with similar devices and systems used for general applications. Most types of problems are represented. However, the number may indicate poor reliability for the PPS application. The LERs do not provide enough details for an in-depth evaluation of the problems. Specific recommendations which would correct AN 2 problems therefore cannot be made in this report. The following list of general items to consider in the design of computer systems for nuclear applications therefore does not necessarily apply to correction of AN 2 problems.

1. Computer hardware problems can be reduced by employing many of the same design techniques used in other parts of nuclear power plant design. Redundant computers with independent power and communication links to critical control elements can reduce the consequences of computer malfunction to the plant.[47] (Redundant computers are used at AN 2.) Fail-safe or fail-certain techniques can be applied depending on the type of failures considered. Diversity can be applied to the computer system by using different types of processors, e.g., minicomputers and microprocessors or processors from different manufacturers.[a] Networking and hierarchical control concepts can be used to support redundancy and diversity. Qualification and burn-in tests should be implemented before the system is placed in service to minimize infant mortality failures.

2. Computer software problems can be reduced in a number of ways. Software can be designed so that it is self-checking by using reasonableness checks and/or redundant computation.[47,48] Fault tolerance and fault detection logic can be implemented in the software to check both computations and communications between software modules. Automatic switchover to spare circuits or devices should be utilized. Software engineering principles can improve software by providing an orderly specification, design, development, qualification, testing, and maintenance cycle.[48]

[a] As systems increase in diversity, there may be a corresponding increase in the operational and maintenance skills required to maintain reliable operation. Thus, diversity should be applied judiciously or system reliability may be degraded.

Diagnostic hardware and software should be implemented. Independent review and testing of the software is an excellent technique for improving software quality.[49] Diversity can be obtained by having independent design organizations develop the redundant software on different computers and in different languages.[a]

[a] As systems increase in diversity, there may be a corresponding increase in the operational and maintenance skills required to maintain reliable operation. Thus, diversity should be applied judiciously or system reliability may be degraded.

REFERENCES

1. C. F. Miller et al., Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants, NUREG/CR-1740, EGG-EA-5388, May 1981.

2. Licensee Event Report (LER) for Month of March 1982, NUREG/CR-2000 ORNL/NSIC-200, Vol. 1, No. 3.

3. Licensee Event Report (LER) for Month of April 1982, NUREG/CR-2000 ORNL/NSIC-200, Vol. 1, No. 4.

4. Licensee Event Report (LER) for Month of April 1982, NUREG/CR-2000 ORNL/NSIC-200, Vol. 1, No. 6.

5. Instructions for Preparation of Data Entry Sheets for Licensee Event Report (LER) File, NUREG-0161, July 1977.

6. D. M. Adams and R. R. Rohrdanz, Preliminary Assessment of Design Issues Related to the Use of Programmable Digital Devices for Safety and Control Systems, July 1982 (Draft).

7. Baltimore Gas and Electric Company, Calvert Cliffs Unit 1, Docket Number 50-317, LER Number Not Given, September 1979.

8. Baltimore Gas and Electric Company, Calvert Cliffs Unit 2, Docket Number 50-318, LER Number Not Given, June 1979.

9. Baltimore Gas and Electric Company, Calvert Cliffs Unit 2, Docket Number 50-318, LER Number 80-013, March 1980.

10. Baltimore Gas and Electric Company, Calvert Cliffs Unit 2, Docket Number 50-318, LER Number 80-44, September 1980.

11. Baltimore Gas and Electric Company, Calvert Cliffs Unit 2, Docket Number 50-318, LER Number 80-046, October 1980.

12. Field Change Request, 80-25, Part of LER Number 80-013.[9]

13. Baltimore Gas and Electric Company, Calvert Cliffs Unit 2, Docket Number 50-318, LER Number 82-022, February 4, 1982.

14. Nebraska Public Power District, Cooper, Docket Number 50-298, LER Number 77-044, August 10, 1977.

15. Duquesne Light Company, Beaver Valley Unit 1, Docket Number 50-334, LER 80-099, November 25, 1980.

16. Arkansas Power and Light Company, Arkansas Nuclear One, Unit 2, Docket Number 50-368, LER Number 79-075, August 22, 1979.

17. Arkansas Power and Light Company, Arkansas Nuclear One, Unit 2, Docket Number 50-368, LER Number 80-080, October 1980.

18. LERs 78-020, 79-004, 79-073, 80-053, and 80-058.

19. Baltimore Gas and Electric Company, Calivert Cliffs Unit 1, Docket Number 50-317, LER Number 81-082, December 9, 1981.

20. Baltimore Gas and Electric Company, Calivert Cliffs Unit 1, Docket Number 50-317, LER Number 81-084, December 15, 1981.

21. Georgia Power Company, Hatch Unit 1, Docket Number 50-321, LER Number 82-002, January 7, 1982.

22. Flordia Power and Light Company, St. Lucie Unit 1, Docket Number 50-335, LER Number 81-052, December 10, 1981.

23. Alabama Power Company, Farley Unit 2, Docket Number 50-364, LER Number 82-015, February 25, 1982.

24. Duke Power Company, McGuire Unit 1, Docket Number 50-369, LER Number 82-020, April 1, 1982.

25. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, July 21, 1980.

26. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Numbers not given, July 24, August 28, and October 8, 1980.

27. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number 80-058, October 1980.

28. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number 82-005, January 28, 1982.

29. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number 82-009, April 1, 1982.

30. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, January 9, 1979.

31. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, January 27, 1979.

32. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, January 28, 1979.

33. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, June 1979.

34. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, August 18, 1979.

35. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, August 20, 1979.

36. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, September 1979.

37. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, December 1979.

38. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, December 21, 1979.

39. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, January 7, 1980.

40. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, January 10, 1980.

41. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, January 23, 1980.

42. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, January 28, 1980.

43. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, July 20, 1980.

44. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, July 30, 1980.

45. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, November 11, 1980.

46. Arkansas Power and Light Company, Arkansas Nuclear One Unit 2, Docket Number 50-368, LER Number not given, November 24, 1981.

47. D. W. Boggs, Fault Tolerant Computer Enhances Control System Reliabilty, Control Engineering, September 1981, pp. 129-132.

48. W. Geiger et al., Program Testing Techniques for Nuclear Reactor Protection Systems, Computer, August 1979, pp. 10-18.

49. R. Glass, Software Reliaiblity Guide Book, Prentice Hall, 1979.

50. M. J. Deutsch, Software Project Verification and Validation, Computer, April 1981, pp. 54-70.

APPENDIX A

SYSTEM DESCRIPTION OF THE ARKANSAS NUCLEAR 2 CPC SYSTEM

APPENDIX A

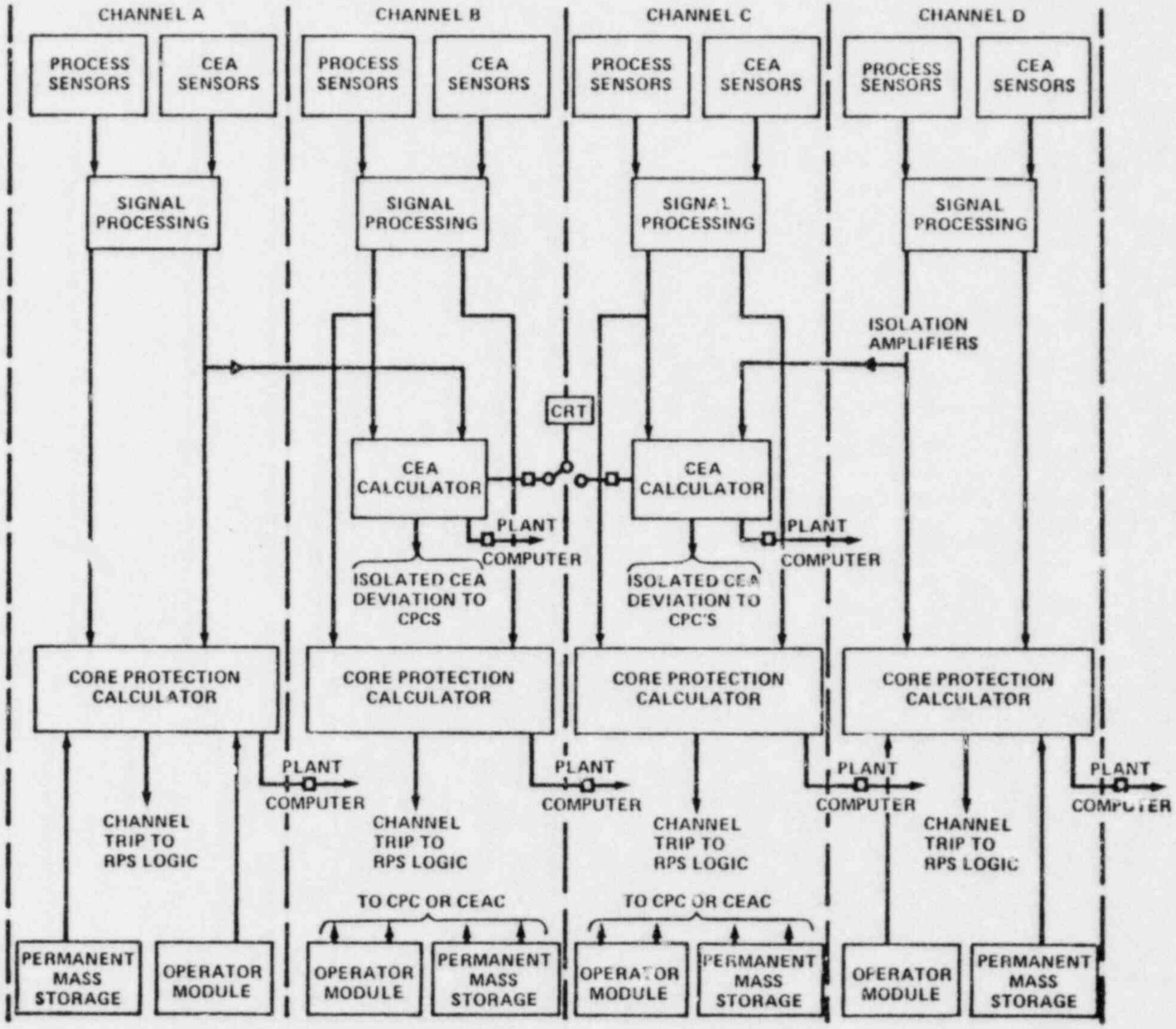
SYSTEM DESCRIPTION OF THE ARKANSAS NUCLEAR 2 CPC SYSTEM

The Arkansas Nuclear 2 (AN 2) CPC System consists of six digital computers configured and implemented to provide protection from low Departure from Nucleate Boiling Ratio (DNBR) and high linear power density. The system, supplied by Combustion Engineering, is composed of four redundant digital computers, referred to as the core protection calculators (CPCs) and two redundant computer based control element assembly calculators (CEACs). The CEACs provide each CPC with processed control element assembly position data. The CPCs acquire data from plant process sensors, the control element assembly position sensors, directly as well as via the CEACs, and perform the required calculations. Each CPC provides trip inputs to one of the four redundant and independent reactor trip system channels when the trip setpoints are exceeded. The functional configuration of the CPCS is shown in Figure 1.

The computers receive both analog and digital input signals. The analog sensor signals are converted to digital signals by means of an analog-to-digital converter. Digital inputs to the computers are received from the operator's modules. The operator's modules are input/output devices to the computers. Each CPC periodically reads the deviation penalty factor communicated from the CEACs.

Each CPC is a byte addressable, 64K byte computer wherein the trip algorithms are implemented and executed. The CEACs are the same type computer, and are used to process control element assembly position information.

The software for the CPCS is functionally structured in terms of modules. These consist of the system executive module, protection algorithm module, initialization module, system test module and the operator's module monitor. The system executive module provides for interrupt servicing, both internal and external, system startup and task



Core Protection Calculator (CPC) System Functional Configuration

Figure A-1

scheduling. Fixed frequency clock interrupts and external interrupts cause execution of the schedule functions, which begins or continues execution of algorithms based on a predefined priority structure.

The initialization module verifies that time-dependent transients have died out of the data and initiates execution of the algorithms stored in memory. The operator's module monitor detects keyboard input, and when in the display mode, updates values of displayed points. Each protection algorithm in the system is priority structured for execution, and is executed at a predetermined frequency.

Finally, the system test module performs automatic on-line testing and provides automatic interface capability for all off-line testing.

Each CPC provides outputs for three continuous displays of calculated results. The displays consist of DNBR margin, local power density margin, and calibrated power based on measured neutron flux. These displays provide the operator with information on the status of each channel.

An operator's module is provided for each protection channel. These are designed to permit the operator to monitor system status, performance, and to enter selected data to the system. The data entered are constants for use in the protection algorithms. These data are called addressable constants and consist of thermal calibration constants, an azimuthal tilt factor, and other data. Each of these constants may vary with time and reactor conditions. Operator input provides a means of updating.

A permanent mass storage unit upon which the protection algorithms, test programs, and test data are stored is provided for each channel. This is the unit from which computer memory is initially loaded or reloaded in the event that it is necessary. The unit is also used during periodic testing of the calculators.