

An Investigation of Digital Instrumentation and Control System Failure Modes

March 2010

Prepared by
K. Korsah
S. M. Cetiner
M. D. Muhlheim
W. P. Poore III

NRC Project Managers
Khoi Nguyen
Thomas Burton

DOCUMENT AVAILABILITY

Reports produced after January 1, 1996, are generally available free via the U.S. Department of Energy (DOE) Information Bridge.

Web site <http://www.osti.gov/bridge>

Reports produced before January 1, 1996, may be purchased by members of the public from the following source.

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone 703-605-6000 (1-800-553-6847)
TDD 703-487-4639
Fax 703-605-6900
E-mail info@ntis.gov
Web site <http://www.ntis.gov/support/ordernowabout.htm>

Reports are available to DOE employees, DOE contractors, Energy Technology Data Exchange (ETDE) representatives, and International Nuclear Information System (INIS) representatives from the following source.

Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831
Telephone 865-576-8401
Fax 865-576-5728
E-mail reports@osti.gov
Web site <http://www.osti.gov/contact.html>

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

**AN INVESTIGATION OF DIGITAL INSTRUMENTATION AND
CONTROL SYSTEM FAILURE MODES**

K. Korsah
S. M. Cetiner
M. D. Muhlheim
W. P. Poore III

NRC Project Managers
Khoi Nguyen
Thomas Burton

March 2010

Prepared for
Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001
NRC Job Code Y6962

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6283
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

	Page
TTLIST OF FIGURES	v
LIST OF TABLES	v
DEFINITION OF TERMS	vii
ABBREVIATIONS AND ACRONYMS	ix
EXECUTIVE SUMMARY	xi
E.1 ANALYSES APPROACH.....	xi
E.2 KEY FINDINGS FROM THE STUDY.....	xi
1. INTRODUCTION	1
1.1 Background.....	1
1.2 Scope and Study Approach.....	1
1.3 Structure of Report.....	1
2. DATABASE SCOPING STUDIES.....	3
2.1 Introduction.....	3
2.2 Databases Reviewed.....	4
2.2.1 Equipment Performance and Information Exchange Database.....	4
2.2.2 Computer-Based Systems Important to Safety Database.....	5
2.2.3 System and Part Integrated Data Resource Database.....	7
2.2.4 FAilure RAte Data In Perspective.....	8
2.2.5 Government-Industry Data Exchange Program.....	8
2.2.6 Aviation Accident/Incident System Database.....	8
2.2.7 Offshore Reliability Data.....	9
2.2.8 Manufacturer Data.....	9
2.3 Results of Scoping Studies.....	10
3. ANALYSES AND CHARACTERIZATION OF FAILURE DATA.....	15
3.1 Analyses of the EPIX Database.....	15
3.2 Generic Software Failure Modes.....	26
3.3 Conclusions.....	28
4. REFERENCES	31
APPENDIX A. TABULATION OF DIGITAL INSTRUMENTATION AND CONTROL FAILURE EVENTS SELECTED FROM THE EPIX DATABASE	A-1

LIST OF FIGURES

Figure		Page
UU1	Generalized computer system in a power plant environment	27

LIST OF TABLES

Table		Page
1	Findings from databases investigated	11
2	Failure modes of cards/modules identified from the EPIX data	17
3	Software failures and causes thereof, as identified from EPIX data (Appendix A).....	18
4	Definition of failure cause as used in this report	21
5	Definition of failure character as used in this report.....	23
6	Failure modes, causes, and characteristics of EPIX digital failure events	23
7	Software system failure modes and software element failure modes	28

DEFINITION OF TERMS

It was recognized early in the course of this study that certain terms relevant to this study are not used in a consistent manner in the technical literature. Thus, in order to provide a consistent framework and basis for any conclusions drawn, definitions of the terms used in this study are provided in this section.

System^{*}—A collection of equipment that is configured and operated to serve some specific plant function (e.g., provides water to steam generators, spray water into the containment, inject water into the primary system), as defined by the terminology of each utility (e.g., auxiliary feedwater system, containment spray system, high pressure coolant injection system).

Component[†]—The structure of a system is what enables it to generate the behavior. From a structural viewpoint, a system is composed of a set of components bound together in order to interact, where each component is another system. This recursion stops when a component is considered *atomic*, i.e., any further internal structure cannot be discerned, or is not of interest and can be ignored. Consequently, the total state of a system is the set of the (external) states of its atomic components.

Equipment—A specific piece of machinery, apparatus, process module, or device used to execute an operation.

Error[†]—An error is a deviation of one or more parts of the system from the correct service state. An error may lead to a system's subsequent service failure.

Failure[†]—A failure occurs when an error is propagated to the service interface and unacceptably alters the service delivered by the system. A failure of a component causes a permanent or transient fault in the system that contains the component. Failure of a system causes a permanent or transient external fault for the other system(s) that interact with the given system.

Failure mode—Failure mode is defined as the way or manner that a failure can occur.

Failure character—For the purposes of this study, failure character is defined as the ensemble of failure modes that exhibit common characteristics.

Failure mechanism—The fundamental processes or phenomena that cause a device to fail through a certain failure mode. For example, processes, such as time-dependent dielectric breakdown, lead to irreversible abnormal conditions that act against the physical process, which provides the basis for performing the intended function of the device.

Failure mechanisms can be considered as the processes that evolve at the very low level of hardware abstraction, e.g., at the device level, which includes the fundamental structures such as transistors, resistors, capacitors, and other subordinate structures such as wires and bonds. For the purposes of this study, failure mechanisms are considered processes that take place below the component level, hence considered outside the scope.

Fault[†]—Fault is the adjudged or hypothesized cause of an error. A fault is said to be *active* when it causes an error; otherwise it is *dormant*.

Module—The definition of module varies widely across industry and engineering disciplines. Within the context of this study, and from our interpretations of the nomenclature recognized by the nuclear industry, a module is regarded as a subsystem, which is a collection of multiple components, that performs specific tasks or functions that are essential for a system in rendering its intended services.

^{*}Source: Industry Guidance for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, NUMARC 93-01, Rev. 2, Nuclear Energy Institute, April 1996.

[†]Algirdas Avinielis et al., Basic Concepts and Taxonomy of Dependable and Secure Computing, Technical Research Report, TR 2004-47, Institute for System Research, University of Maryland.

As an example, a standalone central processing unit (CPU) or microprocessor is considered a component, which relies on certain other components to be able to perform specific tasks or functions. A CPU module, however, contains other supportive and peripheral components such as memory units and communication interfaces. The combined set of components, called a module, can then perform certain functions that are critical steps in delivering the overall function of the system.

It was recognized during the review of the database records, that the phrase “CPU module” is a frequently used name for programmable logic controllers (PLCs).

ABBREVIATIONS AND ACRONYMS

ABWR	advanced boiling water reactor
AIDS	Aviation Accident/Incident System
ASIAS	Aviation Safety Information Analysis and Sharing
ASIC	application specific integrated circuits
AST	asynchronous system traps
CDAS	chemistry data acquisition system
COMPSIS	computer-based systems important to safety
CPU	central processing unit
DI&C	digital instrumentation and control
DOE	Department of Energy
EFM	element failure modes
EMI	electromagnetic interference
EPIX	Equipment Performance and Information Exchange
FMD	Failure Mode and Mechanism Distributions
EPRD	electronic part reliability data
FAA	Federal Aviation Administration
FARADIP	FAilure RAte Data In Perspective
FPGA	field programmable gate arrays
FPLA	field programmable logic array
GIDEP	Government-Industry Data Exchange Program
GIF	Generation IV International Forum
HLD	high-level deficiency
HPCI	high-pressure coolant injection
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
IC	integrated circuit
IDEP	Inter-service Data Exchange Program
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
JLC	Joint Logistic Commanders
LAN	local area network
LLD	low-level deficiency
NAND	NOT AND (logic)
NI	no indication
NPP	nuclear power plants
NPRD	Non-electronic part reliability data
NRC	Nuclear Regulatory Commission
NTSB	National Transportation Safety Board
OREDA	offshore reliability data
PLCs	programmable logic controllers
PLD	programmable logic device
PPCS	plant process computer system
PPI	programmable peripheral interface
PRA	probabilistic risk assessments
RAC	Reliability Analysis Center
RAM	random access memory

RAT	reserve auxiliary transformer
RCIC	reactor core isolation cooling
RFI	radiofrequency interference
RIAC	Reliability Information Analysis Center
SFM	system failure mode
SPIDR	System and Part Integrated Data Resource
SRC	System Reliability Center
SVC	Static VAR compensator
TSLB	trip status light board
ULB	universal logic board
UPS	uninterruptible power supply
VAR	Volt-ampere-reactance
VDC	volts direct current
V&V	validation and verification

EXECUTIVE SUMMARY

This study was conducted to investigate digital instrumentation and control (DI&C) systems—and module-level failure modes—using a number of databases both in the nuclear and non-nuclear industries. DI&C failures from non-nuclear industry databases were included in the investigations because of the potential that such databases might include failure modes of systems/components that are identical to ones used in nuclear applications, such as programmable logic controllers (PLCs). The objectives of the study were to obtain relevant operational experience data to identify generic DI&C system failure modes and failure mechanisms, and to obtain generic insights, with the intent of using results to establish a unified framework for categorizing failure modes and mechanisms.

E.1 ANALYSES APPROACH

Several relevant sources of DI&C failure data were identified, and the databases were assessed for the quality, completeness, and usefulness of the data with regard to the objectives of the study (i.e., whether the databases allow identification of credible failure modes at the system or module level). For the databases that satisfied these criteria, failure modes and failure causes of several DI&C modules were identified. These failure modes were then analyzed to identify any common characteristics, which then enabled some categorizations to be made.

Since information regarding software failure modes from the databases was very sparse, and event descriptions were often not comprehensive enough to identify the software failure mode and/or the cause of the software failure, the data on software failure modes were supplemented by briefly reviewing the literature to document generic software failure modes.

The available data were analyzed to see if a unified framework of failure modes and mechanisms could be established to facilitate meaningful integration of relevant information from multiple sources, with a focus on information that helps characterize failure modes in DI&C systems for operating nuclear power plants (NPPs) and new reactors.

To supplement the data obtained from the database reviews, several attempts were also made to obtain DI&C failure mode data from nuclear power plant instrumentation and control (I&C) manufacturers. These attempts were not successful in obtaining information.

E.2 KEY FINDINGS FROM THE STUDY

Of the seven databases studied, the Equipment Performance Information Exchange (EPIX) database was found to contain the most useful data relevant to the study. Out of a total of 2,263 records, data were retrieved using relevant keywords. Of the 2,263 event records, a total of 226 events were randomly selected and analyzed. One hundred and twenty six (126) of these analyzed events were found to be nondigital-related, and therefore were discarded. Furthermore, a significant number of the remaining 100 events (~35%) were documented in such a manner that identification of the failure mode of the component or system cannot be easily done or is even possible.

The following observations are based on the analyses of the 100 records that were found to be DI&C-related:

- a. About 11% involved application specific integrated circuits (ASICs) and/or field programmable gate arrays (FPGAs).
 - Only ~3% of the failures involved FPGAs, and over 65% of these failures were due to loss of programmed memory of the FPGA. Although the percentage of failures of FPGAs found in the review was very small, it is significant to note, based on the focus of the study (i.e., failure modes of DI&C), that “Loss of Programmed Memory” appears to be a significant failure mode of such devices.

- About 8% of the failure events in the EPIX data analyzed involved ASICs. Failure modes of the ASIC cards included “failed passive components” (e.g., “shorted capacitor”), “failed output” (LO or HI), “shorted operational amplifier,” and “intermittent loss of power.”
- b. About 35% of failures in the EPIX data analyzed involved PLCs. Failure modes included “Loss of Communication,” “Incorrect Firmware Coding,” “Loss of Power,” and “Processor Lockup.”
 - c. The description of some of the events in the EPIX database also contains information on the cause of failure. In many cases, however, the cause of the failure could not be identified or was simply not specified.
 - d. The EPIX database was found to contain little information on software failure modes. Less than 10% of the records analyzed were attributed to software. In addition, event descriptions were often not comprehensive enough to identify the software failure mode and/or the cause of the software failure. Therefore, to supplement the results, a brief review of the literature was performed to document generic software failure modes. These generic software failure modes are documented in Table 7.
 - e. Several of the events among the records analyzed can be considered unique to digital systems. Examples include:
 - A failure in a test program to verify that the wait time for a physical process to complete was long enough is a uniquely digital failure mode in the sense that it is difficult to anticipate and to test the actual functions of a complex system with complete accuracy.
 - The probability of an undetected latent error increases with complexity; complexity is more of a problem with digital systems because it is feasible to automate a complex operation like the optimum fuel handling procedure.
 - Communications present unique problems for digital systems. The ease of changing digital programs is both strength and vulnerability. This is an example of a failure that is not possible for conventional hardwired controls.
 - Similar failures to an intermediate value such as the one encountered in Record 82 exist in the conventional discrete component logic of safety systems. What is different in this case is that the design of the board was sophisticated enough to self-diagnose the failed condition and initiate the alarm light and place the output in the fail-safe state. This appears to be a unique digital failure, but one that worked better than the comparable analog failure.

The lack of quality and detailed information did not allow the development of a unified framework for failure modes and mechanisms of nuclear I&C systems. An attempt was made to characterize *all* the failure modes observed (i.e., without regard to the type of I&C equipment under consideration) into common categories. It was found that all the failure modes identified could be characterized as (a) detectable/preventable before failures, (b) age-related failures, (c) random failures, (d) random/sudden failures, or (e) intermittent failures (see Table 6). However, there was an insufficient number of events related to any one type of equipment (e.g., PLCs, ASIC-based equipment, FPGA-based equipment, etc.) in the records examined to further characterize failure modes of each type of equipment into common “failure characters.”*

Only a small sample size (226) of the 2,263 events was randomly selected for detailed review to evaluate the value of the EPIX database. Because the 100 DI&C-related events that were reviewed (out of 226) identified failure modes that are new and unique and not found in older analog systems, the remaining ~2000 records should be reviewed.

*For the purposes of this study, failure character is defined as the ensemble of failure modes that exhibit common characteristics.

1. INTRODUCTION

1.1 BACKGROUND

There are 104 fully licensed nuclear power reactors in the United States (U.S.).¹ At present, there are also four certified new reactor designs—AP600, AP1000, CE80+, and advanced boiling water reactor (ABWR), with several other designs in the precertification or certification stage.² In addition, the U.S. Department of Energy (DOE) actively participates in the Generation IV International Forum (GIF) that seeks to develop the next generation of commercial nuclear reactor designs before 2030.³ The instrumentation and control (I&C) of these generations of nuclear power plants, including upgrades of current generation of plants (i.e., Gen II and III), are expected to make extensive use of digital instrumentation and control (DI&C). Although the analog systems may have higher overall failure rates compared to digital systems, their failure mechanisms and failure modes are believed to be better understood. Some of the issues that an increased application of DI&C in safety systems pose are (1) the possibility of software or embedded firmware failures compromising plant safety, (2) the probability of a common-cause failure occurring because of software errors, and (3) previously unknown or unrecognized failure modes. These types of failures cannot occur in analog I&C systems.

The U.S. Nuclear Regulatory Commission (NRC) sponsored the study documented in this report to obtain relevant operational experience data (at both the system and module levels) to identify generic DI&C system failure modes and failure mechanisms and to obtain generic insights into DI&C failures, with the intent of using the results to inform the regulatory process.

1.2 SCOPE AND STUDY APPROACH

The databases included in this study are those that contain operational experience data on DI&C equipment failures. To ensure completeness of the study, every attempt was made to include operational experience data from databases maintained by nuclear I&C manufacturers. Unfortunately, none of these efforts yielded any fruitful results. DI&C failure databases from non-nuclear industries, where such databases were judged to include failure modes of system/components that are identical to ones used in the nuclear environment, [e.g., programmable logic controllers (PLCs)], were also included in the study.

The emphasis of the review was on system- and/or module-level failure modes, rather than on device-level (i.e., integrated circuit-level) failure modes. In this regard, relatively few databases matched the criteria. Preliminary scoping studies to down-select a number of potentially useful databases for more detailed analyses also included databases that were later found to almost exclusively contain device-level failure data. These databases [e.g., System and Part Integrated Data Resource (SPIDR)] were not investigated in detail after the preliminary scoping studies. However, findings from the scoping studies with regard to these databases are also included in this report for completeness.

1.3 STRUCTURE OF REPORT

The information presented in this report consists of a review of several failure databases to identify failure modes of DI&C systems. Section 2 describes the scoping studies that were performed on the databases to assess the quality, completeness, and usefulness of the information content. Section 3 describes the analysis of the appropriate databases to identify failure modes and failure causes for both hardware and software. An attempt was also made to characterize these failures in order to establish a unified framework of failure modes to facilitate meaningful integration of relevant information from multiple sources and at multiple levels of physical integration. Section 3.3 summarizes the conclusions of the study.

2. DATABASE SCOPING STUDIES

2.1 INTRODUCTION

This study focused on DI&C failure modes at the module- and system-level, as opposed to integrated-circuit-level failure modes. While integrated-circuit-level failure data are generally available or can be calculated using several sources,* DI&C equipment failure databases that are publicly available in the desired format are comparatively few in number. Vendors conduct extensive testing of products, especially new product lines or major upgrades. Although there may be a large amount of failure data for the products delivered, this information is typically proprietary and is seldom made publicly available. Technical literature in computer reliability and dependability is also a rich source of data. Significant efforts have been made to gain a thorough understanding of how computing platforms fail in general and to establish a common language for defining these failure phenomena.⁴⁻¹⁰ Most of the research in this field considers hardware and software as disparate entities. There are, however, studies that aim at consolidating hardware and software into a single unit of interdependent subsystems.¹¹ Another data source in which digital equipment failure data may be available is facility maintenance records. However, failure mode data from this source may not include all possible component failure modes. Many nuclear power plants (NPPs) maintain maintenance records and use this information to update their probabilistic risk assessments (PRAs). However, licensees do not provide the failure data in their PRAs but instead use the generic failure mode of “fails” (i.e., the component fails to function).

During the preliminary scoping studies to down-select a number of potentially useful databases for more detailed analyses, it was recognized that the majority of the databases reviewed did not contain failure mode data, particularly at the module- and system-level. For instance, SPIDR from Alion Science and Technology Corporation’s System Reliability Center (SRC) claims to have reliability and test data for systems and components. Only after the software and the data library were purchased and investigated was it understood that the database contained failure information solely for integrated circuit devices. The SPIDR database might have system-level failure or reliability data as claimed for other types of systems (e.g., electromechanical), but not for digital systems. Databases that did not specifically address module- and/or system-level failure modes were eliminated from further analysis after the preliminary scoping studies. However, the findings from these preliminary studies have been included in this report for completeness.

The databases that appeared to be candidate sources of DI&C failure mode information were evaluated against the following criteria:

1. Does the database possess the quality and completeness necessary to meet the objectives of the study? For example, are there any limitations such as inconsistency in the reporting across utilities/participating bodies and/or does the database facilitate extraction of failure modes information?
2. Does the database contain failure information on systems or subsystems (such as PLCs, priority modules, etc.)?
3. Does the database contain failure information on DI&C components [e.g., application specific integrated circuits (ASICs) and field programmable gate arrays (FPGAs)] that are likely to be used in NPPs?
4. Does the database contain root cause analyses information?
5. Does the database contain any information on software failures?

*These sources include vendor data, technical literature, facility records, published or private databases, and reliability prediction models.

2.2 DATABASES REVIEWED

2.2.1 Equipment Performance and Information Exchange Database

The Institute of Nuclear Power Operations' (INPOs) Equipment Performance and Information Exchange (EPIX) database contains descriptive reports from U.S. commercial NPPs on component and (safety) system failures. Much of the following information on EPIX is excerpted from Reference 12. Information in EPIX includes input from utility managers, system and component engineers, Maintenance Rule coordinators, reliability engineers, and PSA practitioners. EPIX contains root cause information for failures/occurrences involving components that perform functions in support of systems within the scope of the Maintenance Rule¹³ [NRC Regulations Title 10, Codes of Federal Regulations, Part 50, Section 65 (10 CFR 50.65)] and any other components that cause power reductions or transients.

The data for the EPIX database is supplied by nuclear plant licensees. EPIX output reports available on the INPO Web site currently support the following:

- searches for component-level operating experience to meet emerging site needs,
- identification, prioritization, and root cause analyses of repetitive equipment failures,
- trending of performance and of component and system health reports,
- identification and prioritization of trends in industry/site equipment performance,
- benchmarking,
- exchange of root cause analyses information, and
- required use of industry operating experience, as outlined in NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants."¹⁴

EPIX data are stored in a relational database made up of several tables.¹² Pertinent data fields of the tables are listed below:

- **Device Detail:** unit name, failure report number, component type, piece parts, system name, component model number, failure mode, manufacturer, age at failure, general cause, specific cause, preventive actions, etc.
- **Failure Header:** unit name, failure report number, contact information, reporting criteria, discovery date, report disposition information, etc.
- **Failure Documents:** unit name, failure report number, document title, failure narrative, etc.
- **Function Impact:** unit name, failure number, function impacted, component, piece part, repeat failure, maintenance preventable, functional failure, etc.
- **Repeat Failures:** unit name, failure report number, repeat of previous failure report number, event date of previous event, etc.
- **System Impact:** unit name, failure report number, system name, train designator, repeated event, component, piece part,
- **Unit Effects:** unit name, failure report number, date, unit effect, unit mode, etc.

In addition to being able to search the data tables, the EPIX Web site permits text searches of the event narrative. Boolean logic is supported, and necessary, to identify failures of DI&C more completely and specifically than is available by searching the data fields. Examples of text search topics could include: PLC, programmable, software, hardware, digital, computer, processor, ACIS, FPGA, logic, etc.

2.2.1.1 Data quality and other considerations of the EPIX database

In many cases, the information contained in the EPIX database is insufficient to directly identify credible failure modes down to the component level, or even correctly identify system-level failure. This is because the description of the event and how much detail is provided depends on the individual who is doing the entry. In many cases, the failure mode is not noted, and in any case, the database is not structured to “force” one to provide a description of how the failure affected another system at a higher level, etc. In some cases, the failure of a system or module may be diagnosed down to a circuit board, and the narrative in the database may indicate only that “the circuit card failed.” The mode of failure (e.g., output stuck high or low, intermittent behavior, etc.) is very rarely specified.

An objective of the study was to investigate whether the database contains failure information on DI&C components such as ASICs and FPGAs. The search uncovered relatively few entries on ASICs and FPGAs. Some of these events only indicated that I&C cards containing ASICs and/or FPGAs failed. The particular failure modes of the cards and/or the ASICs and FPGAs were not indicated.

The description of events in EPIX also contains some root cause information. However, in some cases the root cause of a problem is not directly stated. For the purposes of this study, an attempt was made to infer the cause of a failure by studying the narrative describing the incident.

The data reviewed from EPIX contained relatively little information on software failures. About 5% of the failure events* were specifically attributed to software. It is possible that some of the events attributed to failure of the hardware by the reporting utility were actually software related. However, this cannot be validated. One reason why software-related faults might be all too easily attributed to hardware is the fact that software failures are typically caused by “designed-in faults” that react to specific sets of conditions, and typically manifest themselves by some hardware failure (e.g., failure of the digital output to change because of an inherent error in some calculation that only manifests itself under certain conditions).

2.2.2 Computer-Based Systems Important to Safety Database

The Computer-Based Systems Important to Safety (COMPSIS) Project¹⁵ was initiated by a task group formed within the Organization for Economic Cooperation and Development/Nuclear Energy Agency to exchange information on events involving computer-based systems. The overall objective is to improve safety management and the quality of risk analysis of computer-based systems including DI&C systems. The project is envisioned to enable the identification of the root cause of a computer-based system failure, the effect of the failure, and the determination of how the failure could have been prevented. However, the project is relatively new—a first-phase report was published in January 2009, and the study covered only a period of only three years (2005–2007).

The COMPSIS database is designed to collect software and hardware fault experience in computer-based safety-critical NPP systems in a structured and consistent format. This consistent structure is expected to generate insights into the root causes of and contributors to failure events, which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences. The structure is also designed to record event attributes and dominant contributors to these events so that a basis for risk analysis of computerized systems can be established.

In the COMPSIS database, an event is represented as a structured collection of information. Required information for a COMPSIS event is as follows:

- **COMPSIS Event Identifier:** A string that includes Country and Plant Codes, and a National Event Identifier (i.e., provided in the format: Country/Plant Code/National Event Identifier)
- **Title:** A short text chosen to indicate what the COMPSIS event is about.

*Based on 100 records that were found to be digital-related among a total of 226 records reviewed

- **High Level Deficiency Characteristic:** The main classification of the event according to some High-Level Deficiency (HLD) characteristic. This is also a link to allow entry of detailed information about the COMPSIS event.
- **Reported Event:** A link to an entity used to describe the basic event. The data structure for this entity is described in detail in Table 2 of COMPSIS (COMPSIS 2008). Among other things, this data structure includes a description of the event as a whole, and a field for entering a Low-Level-Deficiency (LLD) characteristic.
- **Normal/Low-Level-Event:** An event can be classified as a normal reported event, or as a low-level event. Default values are “Normal.”
- **Additional Information:** Entry of any additional relevant information.
- **Computer-Based Systems:** Definition of the system involved in the event. Defining the system involved in a COMPSIS event is not mandatory. However, once it is decided by the data provider that defining a system is useful for the event description, certain attributes of the system must also be entered. These attributes include the system name, the safety classification, (according to either International Atomic Energy Agency (IAEA) document IAEA NS-G-1.3, International Electrotechnical Commission (IECs) standard IEC 61226, or Institute of Electrical and Electronics Engineers (IEEE) standard IEEE Std 603), the national classification used by the reporting country, classification of the computer-based system according to its function, the safety function of the computer-based system, the failed layer of the system, and the failed element of the system. (The COMPSIS documentation contains tables that define system layers and elements.)
- **Cause Analysis:** An analysis of the cause of the event. The cause analysis can be performed in detail, if available. If detailed analysis is not available, this field is used to give a general indication of the causes behind the event.
- **Corrective Actions:** A description of the corrective actions taken. Defining a corrective action is not mandatory, but once a corrective action is created, other attributes such as “Correction Type” and “Description” of the corrective action are mandatory.
- **Consequence Analysis:** A description of the consequence of the COMPSIS event. As in the case of the “Cause Analysis,” the consequence analysis can be provided in a simplified way in the form of a text description, or in a more structured form by listing and linking the consequences, both observed and potential.
- **Summary:** A brief description of the impact of the COMPSIS event.
- **Severity Level:** Severity level has three attributes: (a) impact on people; (b) impact on facility; and (c) impact on environment.
- **NPP Operational Status:** The operational status can be one of the following: (a) Under Construction; (b) In Operation; (c) Shut Down; (d) Under Decommissioning; or (e) Decommissioned.
- **Plant Condition:** The condition of the facility at the time of the COMPSIS event.
- **Attachments:** Any document that helps in understanding the case can be attached.
- **Lessons Learned:** Instead of giving one text field to freely write lessons learned, the data entry format allows the lessons learned to be organized into a list of simpler lessons.

2.2.2.1 Data quality and other considerations of the COMPSIS database

An important advantage of COMPSIS is that it was specifically designed to collect software and hardware fault experience in computer-based safety-critical NPP systems in a structured and consistent format. As such, the database should provide important information on the subject in the long term. Since the project is relatively new as described previously, it is the opinion of the authors that the database does not yet contain sufficient information to envelop digital hardware/software failure experience and/or failure modes for the NPP environment. However, those relevant findings from the aforementioned COMPSIS report are included in this report.

2.2.3 System and Part Integrated Data Resource Database

Released by the SRC of Alion Science and Technology Corporation, SPIDR contains failure data from multiple sources, including extensive quantitative and qualitative databases on DI&C components from numerous industry and government test and field sources. SPIDR is a replacement of the following Reliability Analysis Center (RAC) data resources:

1. Non-electronic Part Reliability Data (NPRD-95),
2. Electronic Part Reliability Data (EPRD-97),
3. Failure Mode and Mechanism Distributions (FMD-97), and
4. Electrostatic Discharge Susceptibility Data 1995 (VZAP).

Failure mode data appear to be collected from the FMD-97 database. FMD-97 is a cumulative compendium of data consisting of the FMD-91 data along with all the data collected by RAC since 1991. The scope of the document is electronic, mechanical and electromechanical parts or assemblies. The Reliability Information Analysis Center (RIAC), formerly known as RAC, is a Department of Defense Information Analysis Center sponsored by the Defense Technical Information Center.

Failure modes and mechanisms are provided for a large number of I&C components. The SPIDR software system comes as an ensemble of a built-in search engine and the data source. Database queries can be performed using a graphical user interface. The Primary Search Criteria on the input screen provides fields for narrowing the components' specifications. For instance, the keyword "IC: Integrated Circuit" can be entered as a high-level device category name, but narrowed down further by sub-level names such as "Digital," "Memory," "RAM: Random Access Memory," "Dynamic," and "Fast Page Mode." Optionally, additional criteria or output restrictions can be input in the user interface to further narrow the search space. Five different output reports are provided: Failure Rates, Duration Tests, Pass/Fail Tests, Field Failure Modes, and Test Failure Modes.

SPIDR generates a summary output for observed primary failure modes, failure mechanisms, and calculated failure distribution. For certain primary failure modes, a detailed secondary failure mode and failure mechanism data are provided. Primary failure modes are considered the high-level failure category. Allowable field values include Parametric Failure, Functional Failure, Mechanical Failure, etc. Secondary failure mode is a lower level failure mode category than the primary failure mode categories. Allowable field values include Bit Error, Intermittent Operation, Data Word Failure, etc. Failure mechanism is the underlying physical phenomenon that leads to the observed failure mode. Possible field values include Data Bit Failure, Signal Timing Error, Open Bit Locations, etc.

2.2.3.1 Data quality and other considerations of the SPIDR database

SPIDR contains failure mode and failure mechanism data for most digital IC components. Although limited, the database also contains software failure data. SPIDR provides failure data in a well-structured fashion that facilitates querying the data source. Some inconsistencies were found in failure mode

designations, but these deficiencies were mostly attributed to SPIDR being a more generic data source for a wide range of components from mechanical to electrical.

The major “shortcoming” of SPIDR with regard to the focus of this study is that the vast majority of the data contained therein are single I&C devices and no module or system information is provided. SPIDR does contain some failure data on ASICs and FPGAs, components which are also of interest in this study.

Another observation about SPIDR during the scoping study was that some of the “failure modes” reported are not failure modes in the traditional technical understanding of the term, but rather failure causes. In addition, the failure data are mostly from test data, and failure mode data from the field is limited.

The SPIDR database was not selected for further detailed study because of its limitation to device-level failure data.

2.2.4 Failure RAte Data In Perspective

Failure RAte Data In Perspective (FARADIP) was included in the scoping studies because initial indications from the owners of the database were that it was similar to SPIDR and contained module-level DI&C failures data. However, it was concluded after the scoping review that it does not contain any useful information for the purposes of this study. The database does not contain a significant amount of failure mode data—only a small number of DI&C components are listed, with possible failure modes and failure rates. The scoping study did not uncover any DI&C module failures. Therefore, no further analyses of FARADIP were conducted.

2.2.5 Government-Industry Data Exchange Program

Government-Industry Data Exchange Program (GIDEP) began as the Inter-service Data Exchange Program (IDEP) in the late 1950s. Created by mutual agreements of the three military services, i.e., Army, Navy, and Air Force, the purpose of IDEP was to reduce testing being conducted on the same parts, components, and materials. At its inception, IDEP covered only ballistic missile systems developed under U.S. defense programs. In the 70s, the three services of IDEP offices were consolidated by agreement of the Joint Logistic Commanders (JLC), and the program became known as the GIDEP. By request of the JLC, the Navy assumes overall program management of GIDEP.

GIDEP provides a framework for collaborating with government and industry partners to address certain weaknesses of common components. Some integrated circuit manufacturers provide failure data on digital components as part of the exchange program.

The GIDEP database was analyzed for its content. Its structure was not found useful for the purpose of this study and therefore, it was not further considered beyond the scoping studies. The major shortcoming of the database was determined to be an inconsistent reporting structure for the failure data across the reports submitted by the various manufacturers. There was no systematic treatment and classification of the failure modes.

2.2.6 Aviation Accident/Incident System Database

The Aviation Accident/Incident System (AIDS) database is maintained by the Federal Aviation Administration (FAA) and may be accessed through the Aviation Safety Information Analysis and Sharing (ASIAS) System portal.¹⁶ The AIDS database was included in the scoping study because the study was not to be limited to databases in the NPP environment, but it was to also include failure databases in the non-nuclear industries that contained DI&C similar to those used in NPPs (e.g., PLCs).

The AIDS database contains incident data records for all categories of civil aviation. Incidents are defined as “events that do not meet the aircraft damage or personal injury thresholds contained in the

National Transportation Safety Board (NTSB) definition of an accident.” It has a query interface with textual search field that can be used to narrow searches when used in conjunction with all or some of the other data fields provided. These fields are the following:

- Narrative Text
- Report Number
- Event Start Date
- Event End Date
- State
- Airport Name
- Operation Type
- Event Type
- Flight Phase
- Operator Name
- Aircraft Make Name
- Aircraft Model Name
- Aircraft Series

Search words such as “computer,” “software,” “programmable logic controller,” and “PLC,” were used in searching the database. The search of the database yielded little useful information (e.g., using the search term “computer” to find incidents that occurred between 1995 and 2008 yielded 56 records). However, only four of these records were either relevant to DI&C events, or provided information at a sufficient level of detail to enable some level of identification of DI&C failure modes and/or causes to be made. In most cases, the only failure mode/cause information included in the description was something like “flight computer failed,” or “computer failed to initiate signal to release proper break.” A search within the same period (1995–2008) using the keyword “software” yielded only three records, one of which was already included with the records located using “computer” as the keyword. Because of the lack of information regarding failure modes of DI&C equipment likely to be found in the power plant environment (e.g., PLCs) as well as software, no detailed studies were performed on the AIDs database.

2.2.7 Offshore Reliability Data

The Offshore Reliability Data (OREDA) project¹⁷ was established in 1981 and is sponsored by nine oil and gas companies with worldwide operations. The project publishes reliability data for a wide variety of offshore topside and subsea equipment (as well as some onshore equipment) used in oil and gas exploration and production. The project has been publishing reliability handbooks on such equipment since its inception and, at the time of writing, the handbook was in its 4th edition (OREDA 2002).

The majority of the OREDA reliability data covers electromechanical equipment and machinery such as electric generators and motors, gas turbines, compressors, combustion engines, heaters and boilers. However, a section is also devoted to safety equipment (fire and gas detectors and process sensors) and control systems of subsea equipment. A review of the safety and control equipment failure data have been documented in an earlier and related technical report.¹⁸

2.2.8 Manufacturer Data

Four I&C manufacturers were contacted several times in an attempt to obtain relevant I&C failure mode information. There was no response from two of them. Progress with the third manufacturer never progressed beyond the initial discussion stage while interaction with the fourth one stalled over reaching agreement on a non-disclosure agreement in a timely manner.

2.3 RESULTS OF SCOPING STUDIES

Eight databases and handbooks containing failure information were reviewed. Of these, the EPIX and COMPSIS databases were found to contain system- and module-level failure data. The rest (e.g., SPIDR), were found to contain device-level (i.e., integrated circuit-level) failure data. Findings from these databases are summarized Table 1. It can be seen that comparatively, the EPIX database contains the most useful information with regard to the objectives of the study.

Note that five research objectives are identified in Table 1 against which each database was evaluated. For each of these five objectives, three assessments were made as to the amount of information found, completeness of the information, and usefulness of the information. For example, for the EPIX database, there is inadequate information to meet the research objective of identifying/characterizing software failures. Note also that the table uses the qualitative designations of “Adequate,” “Limited,” “Very Limited,” and “Inadequate” to characterize whether or not the information found in the database meets the particular objective of the study. The definitions of these qualitative designations are as follows:

- **Adequate:** Over 60% of the data in the database was found to contain useful information to meet the particular research objective.
- **Limited:** Only 40 to 60% of the data was found to contain sufficient information to meet the particular research objective.
- **Very Limited:** Only 20 to 40% of the data was found to contain sufficient information to meet the particular research objective.
- **Inadequate:** Less than 20% of the data was found to contain sufficient information to meet objectives.

Table 1. Findings from databases investigated
 [See text (Sect. 2.3) for qualitative designations used in the table]

Database	Objective of research	Conclusions			Comments
		Information found?	Data complete (in meeting objective of research)?	Data useful (in meeting objective of research)?	
EPIX	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Limited	Limited	Adequate	In many cases, the specific failure mode and failure cause of hardware/software failures are not specified. At best, the failure of a system or module may be diagnosed down to a circuit board, and the corresponding event description may indicate only that a “circuit card failed.”
	Failure information on digital components (such as ASICs, FPGAs, that are likely to be used in NPPs	Very Limited	Very Limited	Very Limited	
	Root cause analysis information	Very Limited	Very Limited	Very Limited	
	Information on software failures	Inadequate	Inadequate	Inadequate	
	Identification/ of failure modes	Limited	Limited	Limited	
COMPSIS	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Limited	Limited	Limited	Each event in the database is identified with a description and classified according to a “high-level deficiency” characteristic. These recorded events were then later analyzed and classified (by the COMPSIS study group), according to one or more “low-level deficiencies”
	Failure Information on digital components (such as ASICs, FPGAs, that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	
	Root cause analysis information	Inadequate	Inadequate	Inadequate	
	Information on software failures	Very Limited	Very Limited	Very Limited	
	Identification of failure modes	Very Limited	Very Limited	Very Limited	

Table 1. (continued)

Database	Objective of Research	Conclusions			Comments
		Information Found?	Data Complete (in meeting objective of research)?	Data Useful (in meeting objective of research)?	
SPIDR	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	SPIDR has the most failure mode data on various digital components. However, these are at the device/component level rather than at the module or system level and therefore considered outside the scope of the study.
	Failure Information on digital components (such as ASICs, FPGAs) that are likely to be used in NPPs	Adequate	Adequate	Inadequate	
	Root cause analysis information	Inadequate	Inadequate	Inadequate	
	Information on software failures	Inadequate	Inadequate	Inadequate	
	Identification of failure modes	Adequate	Inadequate	Inadequate	
FARADIP	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	FARADIP was found to contain failure mode and failure rate information for only a relatively small number DI&C components.
	Failure information on digital components (such as ASICs, FPGAs) that are likely to be used in NPPs	Limited	Limited	Inadequate	
	Root cause analysis information	Very Limited	Very Limited	Inadequate	
	Information on software failures	Very Limited	Very Limited	Inadequate	
	Identification of failure modes	Very Limited	Very Limited	Inadequate	

Table 1. (continued)

Database	Objective of Research	Conclusions			Comments
		Information Found?	Data Complete (in meeting objective of research)?	Data Useful (in meeting objective of research)?	
Government/ Industry Data Exchange Program (GIDEP)	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	The major shortcoming of the database is that the failure data, in general, is reported in manufacturers' technical reports. Therefore, no consistency was observed within the reporting structure.
	Failure information on digital components (such as ASICs, FPGAs) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	
	Root cause analysis information	Inadequate	Inadequate	Inadequate	
	Information on software failures	Inadequate	Inadequate	Inadequate	
	Identification of failure modes	Inadequate	Inadequate	Inadequate	
Aviation Accident/ Incident Database (AIDS)	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	No information could be found on failure modes of DI&C equipment (including software) likely to be found in the power plant environment.
	Failure information on digital components (such as ASICs, FPGAs) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	
	Root cause analysis information	Inadequate	Inadequate	Inadequate	
	Information on software failures	Inadequate	Inadequate	Inadequate	
	Identification of failure modes	Inadequate	Inadequate	Inadequate	

Table 1. (continued)

Database	Objective of Research	Conclusions			Comments
		Information Found?	Data Complete (in meeting objective of research)?	Data Useful (in meeting objective of research)?	
Offshore Reliability Data (OREDA)	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	The majority of the OREDA reliability data covers electromechanical equipment and machinery such as electric generators and motors, gas turbines, compressors, combustion engines, heaters and boilers. However, a section is also devoted to safety equipment (fire and gas detectors and process sensors) and control systems of subsea equipment. A review of the safety and control equipment failure data has been documented in an earlier and related technical report (see Reference 18).
	Failure information on digital components (such as ASICs, FPGAs) that are likely to be used in NPPs	Inadequate	Inadequate	Inadequate	
	Root cause analysis information	Inadequate	Inadequate	Inadequate	
	Information on software failures	Inadequate	Inadequate	Inadequate	
	Identification of failure modes	Inadequate	Inadequate	Inadequate	
Manufacturer Data	Failure information on systems or subsystems (e.g., PLCs, priority modules) that are likely to be used in NPPs	Attempts to obtain information were unsuccessful			See Sect. 2.2.8 for details.
	Failure information on digital components (such as ASICs, FPGAs) that are likely to be used in NPPs				
	Root cause analysis information				
	Information on software failures				
	Identification of failure modes				

3. ANALYSES AND CHARACTERIZATION OF FAILURE DATA

3.1 ANALYSES OF THE EPIX DATABASE

This section discusses findings from the search of the EPIX database for digital-related event records in detail. Because of the generally scant information on software failure modes, this section also includes information on generic software failure modes identified from a brief review of the literature that was performed to document generic software failure modes.

A table of DI&C failure events selected from the EPIX database is shown in Appendix A. A total of 2,263 files were initially downloaded from EPIX database using the following keywords as search terms:

- PLC
- Programmable AND NOT PLC
- Software
- Algorithm
- ASIC
- Digital
- Computer
- Processor
- Integrated circuit

Out of this total of 2,263 records, a total of 226 events were randomly selected and (manually) analyzed. One-hundred and twenty-six (126) of these analyzed events were found to be nondigital-related and, therefore, discarded. Appendix A provides a summarized listing of findings from the analysis of the 100 events (out of the 226) that were found to be digital-related.

Each record was reviewed to identify the component, module, or system that failed, as well as the failure mode and the effect of the failure either on the modules or systems at a higher level (e.g., the effect of a failure of a component in the safety injection system if the component is part of the safety injection system, or the effect on other systems if those systems are identified in the failure event record). An abbreviated description of the event and the cause of the failure, as identified in the event record, were also reviewed. In Appendix A, an entry of “NI” (No Indication) implies that the relevant parameter was either not explicitly indicated in the event description, or it cannot be unambiguously inferred from the description of the event.

The focus of this study is on module- and/or system-level failure modes. However, because the description of events is not uniform across all records, the failure mode entries in Appendix A sometimes describe failure modes of the failed component and sometimes describe the failure mode of the failed module or system. One example of the former is entry number 3 in the table, as described above. In this case, the failure of (a component on) the logic controller was the cause of the trip. Thus, the failure mode entry refers to the (component on) logic controller. On the other hand, an example of an entry in Appendix A, in which the failure mode entry refers to a module or system, is entry number 81. The “System” is the Plant Process Computer System (PPCS), and the failure mode is the loss of communication to the PPCS.

Several observations were made in the course of the analyses of the data and are also reflected in the Appendix A table. The following observations are based on the analyses of the aforementioned 100 records that were found to be DI&C-related:

- A significant number (~35%) of events are documented in such a manner that identification of the failure mode of the component or system is not easily identifiable or even possible. Entry 3 in the table is typical of such descriptions. This entry describes troubleshooting for the cause of a trip of

the Reserve Auxiliary Transformer (RAT) Static Volt-ampere-reactance (VAR) Compensator (SVC). The cause of the trip was traced to the failure of the logic controller card of the thyristor-switched capacitor bank for the RAT. The description enables one to identify the cause of failure as a “component failure” on the logic card, but the failure mode of the component is not stated. In this case, the entry in Appendix A for the “Failure Mode” is simply “Failure of subcomponent on controller logic circuit card.” In cases where no failed component is identified in the database, the corresponding entry in Appendix A is simply “NI.”

- While some entries appear to be duplicates (e.g., entries 71 and 72), they are actually similar events that occurred at different units and/or at different times. Examples include entries 59 through 61 (involving a reactor water cleanup system), and entries 71 and 72 (involving a containment atmosphere radiation monitoring system).
- Very few events were found to involve FPGAs or field programmable logic arrays (FPLAs).^{*} Only ~3% of the failures involved FPLAs, and over 65% of these failures were due to loss of programmed memory of the FPLA. Although the percentage of failures of FPLAs/FPGAs found in the review was very small, it is significant to note, based on the focus of the study (i.e., failure modes of DI&C), that “loss of programmed memory” appears to be a significant failure mode of such devices.
- About 35% of failures involved PLCs. Failure modes included “loss of communication,” “incorrect firmware coding,” “loss of power,” or “processor lockup.” Failure modes of specific I&C modules (e.g., PLCs, ASICs) identified in Appendix A have been extracted from that table and assembled in a more concise manner in Table 2.
- Only 8 records (record numbers 92 through 99) were identified using the keyword “ASIC.” All of these records involved the 7300 system ASIC-based replacement modules by Westinghouse.¹⁹ Each 7300 replacement module is a card-for-card replacement for previous 7300 (analog) installations.[†] Although it is primarily a card-for-card replacement, it can also be adapted to a card-for-multifunction replacement. The 7300 system main board functions include power supply and distribution, input signal conditioning, analog outputs, and digital actuation outputs. ASIC-based replacement modules available for 7300 system applications can be found in Reference 19. Failure modes of the ASIC cards included “shorted capacitor,” “failed output (LO or HI),” “shorted operational amplifier,” and “intermittent loss of power” (see Table 2).
- About 15% of failures involved power supplies, including uninterruptible power supplies (UPS). A significant portion of these failures was apparently due to aging components. Failure modes included “shorted capacitor” and “erratic output.” A full list of the failure modes identified is shown in Table 2.
- About 10% of the failures could be attributed to software. Here, a word of caution needs to be noted. In many cases, it is difficult to exclusively identify a failure as software-related, since the software is an integral part of a module or system (e.g., PLC). For example, “loss of communication” to/from a PLC may be listed as a PLC failure but could have been due to buffer overflows originating from a latent (software) design flaw. In this study, this is especially true where inadequate analysis of the cause of the problem has been performed by the plant. In studying the EPIX database for software failure modes, a “system-centric” view of software failure has been adopted.

^{*} Although they are referred to as FPLAs in the EPIX database, the more popular term used is FPGA.

[†] The “7300” is designed for process protection and control systems.

Table 2. Failure modes of cards/modules identified from the EPIX data

I&C System, Module, or Component	Failure modes identified from EPIX data (Appendix A)
PLC	Loss of communication Processor lockup Communication timeout Loss of power Incorrect firmware coding Open fuse Unable to reset False output Communication dropout Incorrect functioning of central processing unit (CPU) clock Loss of DC power Failed output (HI or LO) Damaged component Failed to reboot Failed to establish communication Programming error/latent fault in PLC logic
ASIC Card/ASIC-based Module	Shorted capacitor on card Failed output (LO or HI) Degraded pulse-to-analog converter signal Shorted operational amplifier Intermittent loss of power Drift high Drift low Erratic output
FPLA	Loss of programmed logic
Programmable Logic Device (PLD)	Incompatibility with clock speed.
Power supply, UPS, Battery	Open fuse Loss of DC power Damaged capacitors/components Shorted capacitor Erratic output

Table 2. (continued)

I&C System, Module, or Component	Failure modes identified from EPIX data (Appendix A)
Other hardware	Timebase fault Degradation of UPS battery Failure of subcomponent on controller logic circuit card. Unresponsive (lock up of) Programmable Peripheral Interface (PPI) Output out of tolerance (drifting) due to unstable clock Degraded output (due to static buildup) Failed output of address decoder chip Failure to communicate data to remote computer Short circuit Erratic/fluctuating output Network switch disconnected Instrument air pressure drop Loss of communication Damaged capacitors/components Open circuit/loss of continuity Communication interruption (lasted 36 seconds) Communication lockout due to accumulation of timeout errors Spurious performance (isolator card) Erratic output Loss of memory Output card failed high Spurious performance (CPU board) Unresponsive to input command NAND gate output failed in a quasi-trip state (would not provide true "HI") Intermittent loss of power Failed output (HI or LO) Loss of communication

The literature on digital software acknowledges two main interpretations of the concept of software failure.¹⁸⁻²² In the "software-centric" view, the software is considered in isolation, and not as part of the system or equipment in which it operates. Thus, a software failure is a property of the software itself. On the other hand, the "system-centric" view states that the idea of software failure is only meaningful when discussed within the context of the system within which the software operates. The types of software failures identified from the EPIX database are shown in Table 3.

Table 3. Software failures and causes thereof, as identified from EPIX data (Appendix A)

Incomplete description of requirements Incorrect firmware coding Faulty calculation in program Requirements error Incorrect interpretation of requirements Task/Application crash Inadequate software version control Software update incompatible with the Plant Process Computer design basis Inadequate software validation and verification (V&V) Software lockup
--

Several of the events among the records analyzed can be considered unique to digital systems. However, the following were identified as particularly interesting from the records analyzed (see Appendix A):

Record No. 22

Reactor operations took the condensate demineralizer off-line to backwash and precoat per Chemistry Department's direction. However, backwash did not start when the CYCLE START push button was pressed. With operation's permission, the manual start was taken to Step 1 by a technician. This moves the PLC software program to Step 1. Then the technician took the manual start to Step 2. The display was checked and the system was working properly.

The "relay race" causes the very first step to be out of sequence, and subsequently, the machine does not know where it should be. (NOTE: The entry in EPIX defines this as the "relay race.")

The race condition can also occur in relay logic, so it is not uniquely semiconductor logic. The summary does not say, but based on the symptoms, the likely race was a PLC timer that waited for a physical process to complete. The error was that the wait time was not sufficient. The PLC went to a failure mode when the timer expired without completion of the task. In other words, the "race" was between the plant and the controls. This would be a failure in the test program to verify that the wait time was long enough. This is a uniquely digital failure mode in the sense that it is difficult to anticipate and to test the actual functions of a complex system with complete accuracy.

If the race was actually in the PLC logic alone (unusual), then the error was in the design. Analytical techniques are available to eliminate the race condition in Boolean logic, so it should not have happened.

Record No. 23

A refuel platform trolley moved in the wrong direction while the refuel platform was moving toward a core bundle location. The move was being made in the automatic mode. During the move, the bridge was moving at the extreme north end of the core. It should have moved east to the required core location, but it moved west. The safety travel interlock zone was entered and the bridge/trolley was stopped. Safety travel override was used to move away from the northwest corner of the core/vessel, and the move was completed in manual mode.

No root cause is identified. Because the move was completed in manual mode after automatic mode conducted the bridge in the wrong direction, one would deduce that the power control relays and motor controls on the bridge transport are in operation and that the problem is more likely in the automatic control program. The bridge control is a very long sequence of x-y positioning moves of the bridge and the gantry. The problem is very likely related to the complexity of the program that predetermines the bridge movements. The sequence of moves is unique for each refueling. The sequence is also very long and thus hard to verify manually. Because the refueling operation only occurs every 1.5 to 2 years, the automatic bridge control program does not receive extensive usage. These factors combine to give a high probability that a latent failure remains in the design of the control program after testing and that the error is detected during operation. This event is an example of the probability of an undetected error increasing with complexity. Complexity is more of a problem with digital systems because it is feasible to automate a complex operation like the optimum fuel handling procedure.

Record No. 68

An engineer installed software on the Chemistry Data Acquisition System (CDAS) server from the business local area network (LAN) to conduct a test to verify connectivity to the CDAS server and transmit condensate demineralizer values. The Condensate Demineralizer PLC was connected to the plant network and the test was conducted. The software suite was furnished with support services

such as automatic synchronization that identified other existing copy of the software on the local network and performed updates if necessary. Unknown to the software engineer, the software suite established a communication path from the CDAS server through the firewall to the production Condensate Demineralizer personal computer (PC). The test software had all the functionalities, but the system-specific operational parameters were all zeros. The Condensate Demineralizer PLC tags that included operational parameters were overwritten by the zeros in the test suite, which resulted in 0% flow demand—essentially complete isolation of condensate flow to the feedwater system. The isolation caused automatic scram of the reactor on low reactor water level. Eventually, Reactor Core Isolation Cooling (RCIC) and High-Pressure Coolant Injection (HPCI) systems initiated and recovered the reactor water level.

This event highlights the observation that complexity of digital I&C systems may result in failures that cannot be easily anticipated from a top-level understanding. Although the control system in the example was used in a nonsafety-related system and did not have paths for communicating directly with a safety-related system, the high degree of coupling between the systems resulted in initiation of multiple plant protection systems to bring the reactor to a safe and stable condition.

This failure involves a failure in the test procedure and several failures in a communications system design. The controls in place to prevent events such as this include:

- the system design should have precluded an inadvertent software change,
- the test procedure should have isolated the system under test so that it is not connected to a network,
- the communications system should have several places that check for valid messages, particularly those that modify control software,
- the firewall should have been designed to prevent instructions to change software or constants to pass through while the system is in operation,
- the synchronization software should have been designed to target a specific computer, and
- both sending and receiving computers should validate that the software update is from a valid sender, that the receiver is the intended target, and that the receiver is in a state that it is permitted to change instructions or data.

Communications present unique problems for digital systems. The ease of changing digital programs is both strength and vulnerability. This is an example of a failure that is not possible for conventional hardwired controls.

Record No. 82

An annunciator, trip status light board (TSLB) light, and computer alarm actuated, indicating a 1B Steam Generator Steam Line High Delta P Alert. First, it was thought that the symptom was due to a failed channel. Troubleshooting determined that the failure was due to a failed ESFAS—Train A logic circuit. Initial bench testing of the Universal Logic Board (ULB) showed that the card's 2 of 3 logic circuit initiated a trip signal when either redundant channel was in a tripped state. Upon further investigation of this ULB card failure, it was found that a NAND gate in the logic circuit had failed in a quasi-trip state. The output of the failed NAND gate would not allow a true HI (> 7.5 VDC). Although the NAND gate would not provide a true HI, it would provide a 7.0–7.2 VDC output. This degraded output was high enough for the failed ULB to place itself in a fail-safe condition. The Z8 chip being pulled low resulted in the annunciator, TSLB light, and computer alarm to actuate/illuminate.

The failure modes and causes of these failures for all the 100 EPIX records examined were further analyzed in an attempt to identify common characteristics for particular sets of failure modes. Table 4 provides definitions of the “Cause of Failure,” as defined for the purposes of this report. The

causes of failures were either directly obtained from a description of the failure event, or they were inferred as

Table 4. Definition of failure cause as used in this report

Failure cause	Definition
Incompatibility of hardware	A failure primarily due to the fact that some components or subsystems using one technology interface with other components or subsystems that use incompatible technology or design. An example is a design that incorporates faster IC chips with slower ones.
Programming error	A failure resulting from an error in the system software or firmware.
Incomplete requirements description.	A failure resulting from the fact that an undesirable system behavior that could have been avoided by an improved program or logic design was not anticipated, and therefore was not made part of the requirements at the beginning of the system design.
Operating outside of specification	A failure resulting from the fact that the failed system was operating outside of specifications (e.g., high voltage surge caused by lightning, electromagnetic/radiofrequency interference (EMI/RFI) induced faults, etc.).
Incorrect interpretation of requirements	A failure caused by a design error, but the primary cause of which can be traced to an incorrect interpretation of requirements.
Unknown	Self-explanatory.
Human error	A failure due to an unauthorized function performed by a human.
Incompatibility of Software	A failure due to the fact that a software version installed in a module is not compatible with a software version in another module that the first module has to communicate or interact with.
Inadequate software V&V	A failure due to a programming error, but attributed to the fact that the error could have been detected if adequate V&V (e.g., adequate testing) was performed before system was placed in service.
Installation error	A failure due to an error or errors during installation (e.g., ignoring to install the hardware in the required configuration)
Hardware/Software Design Flaw	A failure that is traceable to an error in the design of the hardware and/or software.
Inadequate Environmental Control	A failure due to operating outside environmental temperature and humidity specifications.
Inadequate Software Version Control	A failure caused by inadequate software version control
Corrosion	A failure caused by corrosion.

the most likely cause based on the description of the failure event. The failure modes and their causes were further grouped into “Failure Characteristics” as defined in Table 5. The categorization based on these definitions is shown in Table 6. Note that the number of failure mode entries in Table 6 is less than the number of records in Appendix A. This is because (1) some of the failure events in Appendix A were not described in sufficient detail as to clearly identify the failure mode, and such records were eliminated from further review; and (2) some failure events (as well as the cause of such failures), while they occurred at different times, were found to be identical. Such entries in Appendix A were also excluded from Table 6.

The failure mode is clearly identifiable from the description as a hardware failure on the logic board in which the output failed to an intermediate value. Similar failures to an intermediate value exist in the conventional discrete component logic of safety system. What is different in this case is that the design of the board was sophisticated enough to self-diagnose the failed condition and initiate

the alarm light and place the output in the fail-safe state. This appears to be a unique digital failure but one that worked better than the comparable analog failure.

Table 5. Definition of failure character as used in this report

Failure character	Definition
Execution-sequence-dependent	Failures that typically occur because an expected <u>sequence</u> of events does not occur in the order expected. Examples are communication timeouts, failure of a network node to acknowledge receipt of data, data corrupted in transit (which has to be resent), etc.
Data-dependent	Failures that typically occur due to erroneous data fed to the malfunctioning module from another module. An example is wrong trip/no-trip calculation from one module fed into a voting logic module.
Detectable/preventable faults before failure	Failures that they are likely to be detected before they occur, such as by online monitoring, exhaustive testing prior to installation, adequate configuration control or verification and validation, etc.
Intermittent failure	Failures that appear and disappear seemingly at random.
Persistent failure	Failures that they occur in the same module or system at different times and under the same conditions.
Sudden failure	Failures that they occur comparatively rapidly (as opposed to gradual degradation or age-related failure).
Degradation/age-related failure	Self explanatory. Examples include wear out or drift.
Random failure	Failures that they do not appear to have any pattern or regularity.
Systemic failure	Failures that they are related deterministically to a certain cause or causes.

Table 6. Failure modes, causes, and character of EPIX digital failure events

Failure mode	Failure cause	Failure character
CPU lockup	Incompatibility of hardware	Detectable/Preventable before failure
Incorrect firmware coding	Programming error OR Requirements error/misinterpreted requirements	
Unresponsive in auto mode.	Incorrect interpretation of requirements	
Failure to communicate data to remote computer	Programming Error	
Encoder Output Error		
Instrument air pressure drop		
Task crash [Loss of asynchronous system traps (AST)]	Programming Error OR Incomplete Requirements Specifications	
Faulty program calculation	Requirements error	
Loss of communication (PLC)	Requirements error / Incomplete requirements description OR Misinterpreted Requirement	
Erroneous/false output	Human error	
Open breaker		
Loss of communication	Inadequate software V&V	
Erratic/unstable output		
Incorrect PLC output		
False output	Requirements error OR Incorrect interpretation of requirements	

Table 6. (continued)

Failure mode	Failure cause	Failure character	
Software lockup	Programming error OR Requirements error		
Communication lockout due to accumulation of timeout errors	Programming error AND/OR Operating outside specifications		
PPI unresponsive (lock up)	Operating Outside of Specifications		
Loss of communication			
Spurious performance (CPU board)			
NAND gate output failed in a quasi-trip state (would not provide a true "HI")			
Open fuse (caused by voltage spike)			
Failed to establish communication	Installation error; also operating outside of specifications		
Degradation of battery	Degradation/Age-related	Age-Related	
Voltage regulator card failed due to aging			
Degradation of UPS battery			
Out of Tolerance (drifting) due to unstable clock			
Short Circuit			
Incorrect functioning of CPU or clock			
Loss of Vdc power			
Failure of Control Rod Element Assembly to move specified distance on command.			
Electrolytic capacitor failure (Actual mode of failure not specified)			
Damaged capacitors (mode of failure not indicated)			
Damaged components on output cards (actual failure mode not indicated)			
Spurious performance (isolator card)			
Intermittent Loss of Power			Equipment Aging
Loss of Communication/ Common bus failure			Corrosion
Degraded pulse-to-analog converter signal	NI		

Table 6. (continued)

Failure mode	Failure cause	Failure character
Output degradation (due to static buildup)	Operating Outside of Specifications	Random
Erratic/fluctuating	Unknown	
Unable to reset	Unknown	
Communication Dropout/Loss of communication	Unknown	
Erratic Output	Unknown	
Component failure (actual failure mode not indicated)	Unknown	
Variable Frequency Drive controls failed (mode of failure not indicated)	Excessive traffic (interference or data storm) on the connected plant network	
“Open circuit/loss of continuity”	NI	
FPLA failed (mode of failure not indicated)	Unknown	
Tracking driver card output failed high	Unknown	
Loss of logical network connection	Operating beyond limited software resources	
No output indication	NI	
Communication Dropout	Maximum accrued timeouts	
Failed output of address decoder chip	Unknown	
Failed Output (high or low)	Unknown	
Network switch disconnected	Loss of power	
Unscheduled clock reset	Memory corruption of recorder software	
Computer lockup	Unknown	
PLC failed to reboot	Unknown	
Loss of memory	Battery failure	
Failed analog input card	Unknown	
Processor hang up	Unknown	
Shorted capacitor	Electronic component failure	
Shorted operational amplifier. Overpressure Delta-T setpoint failed high.		
Failed output (HI or LO)	Cold/bad solder joint	
Loss of trip signal	Failure of rotary switch or relay	
Periodic processor hang-up	Inadequate environmental control	Intermittent

A review of Table 6 shows that about 34%* of the failure modes were characterized as detectable/preventable faults, indicating instances where failures that could possibly have been prevented with improved configuration control, improved V&V prior to system development, or perhaps improved test coverage during the V&V procedures and acceptance testing procedures. Note that failures caused by “operating outside of specification” were included in this category.

*Based on the 100 records that were found to be digital I&C-related out of the 226 records reviewed

Twenty three percent of the failure modes were characterized as “age-related.” It is interesting to note that while many of the subsystems that failed in these cases are parts of digital-based systems (e.g., radiation monitors), the majority of the components that failed were power supplies or components related to power supplies. The failure mode was usually a degraded output voltage or an outright power supply failure.

Twenty one percent of the failure modes were characterized as “random,” meaning that these failure modes did not appear to have any pattern or recurrence.

Nineteen percent of the failure modes were characterized as “random/sudden,” meaning that these failures were random and occurred comparatively rapidly (as opposed to gradual degradation). They were characterized differently from just being characterized as “random” because the sudden nature of the failure event could be more readily inferred from the even description in the EPIX database.

Only about 2% of the failure modes were characterized as “Intermittent.”

3.2 GENERIC SOFTWARE FAILURE MODES

As indicated in the previous section, less than 10% of failures in the EPIX data analyzed were attributed to software. In addition, event descriptions were often not comprehensive enough to identify the software failure mode and/or the cause of the software failure. Therefore, to supplement these results obtained by analyzing operating experience from EPIX, a brief review of the literature was performed to document generic software failure modes. This information was obtained from a review of References 20, 21, 22, and 23.

First, it should be noted that definitions of software failure mode, failure cause, and failure effect are not uniformly defined in the literature. This poses some difficulty in attempting to glean insights into software failures and their potential mitigation. Also, definitions that are comparable to those typically used for hardware are desirable to more directly support integration with current PRA models. In general, definition of a software failure mode depends on the level of detail at which the software is being evaluated. For example, buffer overflow leading to failure of communication is a device level software failure mode, which could eventually lead to a system level failure at the NPP. Software may be broken down into several elements wherein each performs one of the generic software functions: input, output, processing, communication, and resource allocation²². The software can be thought of as a system, i.e., a “software system” consisting of “software elements” performing the generic software functions. Two software system failure modes (SFMs) may be defined:²²

(1) **Malfunction of software during execution.** In this situation, the software may stall and stop generating any output because (a) it has run into an infinite loop or (b) it has deadlocked between processes. OR, the software may run as usual but will generate incorrect outputs. Each of these categories [(a) and (b)] can be further divided into two other system level failure modes depending on whether the failures are detectable (e.g., via an error message) or undetectable. Thus, four types of software failure modes during execution can ultimately be identified:

- halt/termination with a clear message,
- halt/termination without a clear message,
- runs with evidently wrong results, and
- runs with wrong results that are not evident.

(2) **Problematic, confusing, and less informative man-machine interface designs.** In this situation, the software runs with misleading commands to the user. The software may provide an incomplete or incorrect display of information, may not provide an alarm when it should, and may provide a nonconservative output. Basically, the software either (a) performs its intended functions successfully but contributes to human errors or (b) fails to display the information correctly. Thus, two types of software failure modes can ultimately be identified:

- software runs with incomplete or incorrect display of information, requiring the operator to take action, and
- software provides the operator with misleading commands.

In general, failure modes and effects analyses are performed at the system- and module-levels in NPPs. The software system-level failure modes identified above contribute to the overall analyses at the system level. However, to conduct a detailed failure analysis, a lower level of detail is required. To facilitate such analyses, the concept of software element failure modes (EFM) has been postulated,²² in which any software package can be divided into only three elements that perform the software's generic functions:

- **Data Input:** Generally, a digital system's software takes input data from the hardware. The data may be pre-processed during input before any computational processing is performed by a subsequent module.
- **Data Processing and Resource Utilization:** During this phase, the input data are processed. During the execution of the software, resources are utilized (e.g., use of CPU time). In addition, there may be intercommunication among various software processes.
- **Data Output:** After processing, the software outputs the results of the data either to another subsystem, an actuator, or for display to an operator.

The scenarios discussed above are similar to the generic computer hardware system of Fig. 1, (Reference 18), in which the software, if viewed as a single package, may be

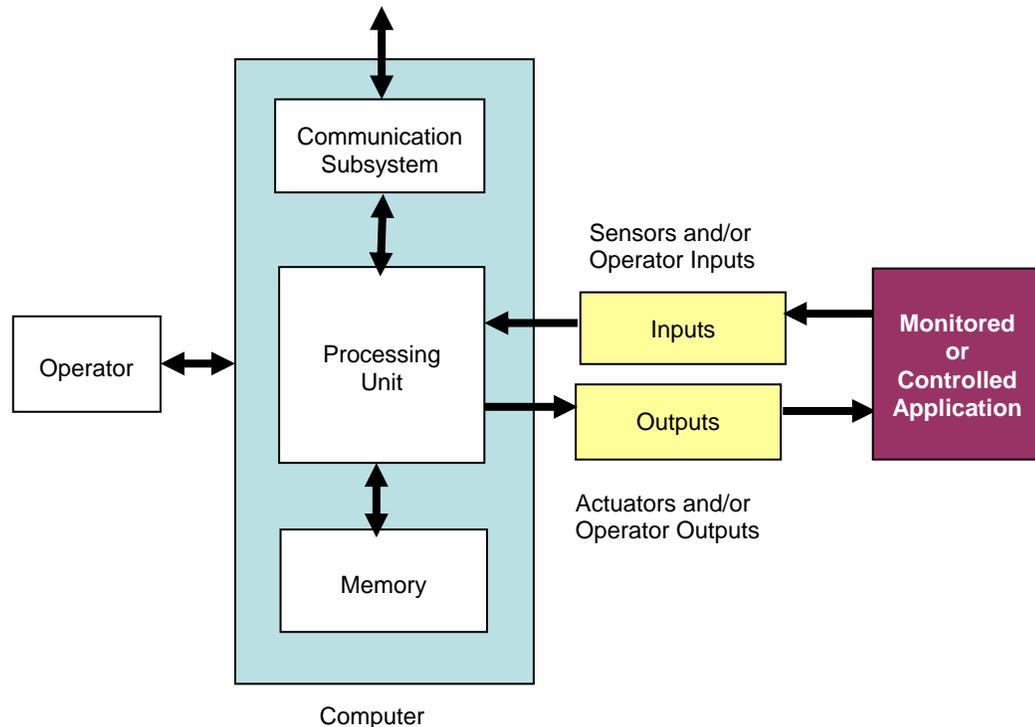


Fig. 1. Generalized computer system in a power plant environment. (Source: Industry Survey of Digital I&C Sources.)

assumed to be part of the box labeled “processing unit.” Accordingly, functional decomposition of the software yields the five elements of **input, output, resource allocation, communication, and processing**. The following generic software failure modes are applicable to all the elements:

- Timing/order failure: a failure mode category that represents the incorrect timing and ordering of events. Examples include execution time exceeding a time limit, incorrect timing of available data, slow response, and incorrect rate of data processing, and incorrect duration of data for processing.
- Interrupt induced failure: a failure category that represents interrupt-induced failures. Examples include incorrect interrupt or service requests.
- Omission of a function or an attribute: this mode represents a function or its attribute that is left out but should have been included.
- Unintended function or attribute: a failure category that represents unintended actions or attributes. which were implemented. Examples include modifying code memory and modifying variables that should not be modified.
- Incorrect implementation of a function or an attribute: a failure mode category that represents a function or an attribute of it that is not left out but is incorrectly implemented.
- Data error: this category represents errors related to data. Examples²³ include incorrect amount, value, range, or type, absent data, or corrupted data.

These failure modes are applicable to all software elements. However, there are also some known, unique failure modes for resource allocation and communication elements. These specific failure modes include loss of synchronism, deadlock, lockout, and interruption and priority error.

The software system failure modes and software element failure modes discussed above are summarized in Table 7.

Table 7. Software system failure modes and software element failure modes
(Adapted from Reference 22)

Software system failure modes	Generic software element failure modes
<ul style="list-style-type: none"> • Halt/abnormal termination <u>with</u> clear message. • Halt/abnormal termination <u>without</u> a clear message. • Runs with evidently wrong results • Runs with wrong results that are not evident. • Incomplete or incorrect display of information requiring operators to take action. • Misleading command to the user. 	<ul style="list-style-type: none"> • Timing/order failure. • Interrupt-induced failure. • Omission of a required function or attribute. • Unintended function or attribute in addition to intended ones. • Incorrect implementation of a function or attribute, • Data error that software logic cannot identify and reject.

3.3 CONCLUSIONS

This study reviewed seven databases* for information on DI&C failure modes and failure causes, and characterized the various failure modes into a few categories in an attempt to establish a unified framework of failure modes and mechanisms to facilitate meaningful integration of relevant

* Attempts were made to also include manufacturer databases. However, these attempts were unsuccessful (see Sect. 2.2.8).

information from multiple sources. With regard to the objectives of the study, the EPIX database was found to contain the most useful data of all the databases reviewed. Even so, a significant number (about 35%) of events were documented in such a manner that identification of the failure mode of the component or system is not easily identifiable or even possible. The COMPSIS database structure was also found to be the most potentially useful, because it allowed events involving DI&C to be documented in a more structured manner. However, the database is relatively new and at the time of this study, there was little information on DI&C failure modes.

Key findings from the analyses of the EPIX database are based on the analyses of the 100 records that were found to be DI&C-related (out of a total of 226 records randomly selected from the 2,263 events retrieved using relevant keywords as discussed in the text):

1. Several of the events among the records analyzed can be considered unique to digital systems. Examples include:
 - A failure in a test program to verify that the wait time for a physical process to complete was long enough is a uniquely digital failure mode in the sense that it is difficult to anticipate and to test the actual functions of a complex system with complete accuracy.
 - The probability of an undetected latent error increases with complexity; complexity is more of a problem with digital systems because it is feasible to automate a complex operation like the optimum fuel handling procedure.
 - Communications present unique problems for digital systems. The ease of changing digital programs is both strength and vulnerability. This is an example of a failure that is not possible for conventional hardwired controls.
 - Similar failures to an intermediate value such as the one encountered in Record 82 exist in the conventional discrete component logic of safety systems. What is different in this case is that the design of the board was sophisticated enough to self-diagnose the failed condition and initiate the alarm light and place the output in the fail-safe state. This appears to be a unique digital failure, but one that worked better than the comparable analog failure.
2. Of the records analyzed, only ~3% of the failures involved FPGAs and over 65% of these failures were due to loss of programmed memory of the FPGA. Although the percentage of failures of FPGAs found in the review was very small, it is significant to note, based on the focus of the study (i.e., failure modes of DI&C), that “loss of programmed memory” appears to be a significant failure mode of such devices.
3. About 8% of the failure events in the EPIX data analyzed involved ASICs. Failure modes of the ASIC cards included failed passive components (e.g., “shorted capacitor”), “failed output (LO or HI), “shorted operational amplifier,” and “intermittent loss of power.”
4. About 35% of failures in the EPIX data analyzed involved PLCs. Failure modes included “loss of communication,” “incorrect firmware coding,” “loss of power,” and “processor lockup,” as well as failure modes of specific I&C modules (e.g., PLCs, ASICs).
5. The description of some of the events in the EPIX database also contains information on the cause of failure. In many cases, however, the cause of the failure could not be identified or was simply not specified.
6. The EPIX database was found to contain little information on software failure modes. Less than 10% of the records analyzed were attributed to software. In addition, event descriptions were often not comprehensive enough to identify the software failure mode and/or the cause of the software failure. Therefore, to supplement the results, a brief review of the literature was performed to document generic software failure modes. These are documented in Table 7.

The lack of quality and detailed information did not allow the development of a unified framework for failure modes and mechanisms of nuclear I&C systems. An attempt was made to characterize *all* the failure modes observed (i.e., without regard to the type of I&C equipment under consideration) into common categories. It was found that all the failure modes identified could be characterized as (a) detectable/preventable before failures, (b) age-related failures, (c) random failures, (d) random/sudden failures, or (e) intermittent failures (see Table 6). However, there was an insufficient number of events related to any one type of equipment (e.g., PLCs, ASIC-based equipment, FPGA-based equipment, etc.) in the records examined to further characterize failure modes of each type of equipment into common “failure characters.”*

Only a small sample size (226) of the 2,263 events was randomly selected for detailed review to evaluate the value of the EPIX database. Because the 100 DI&C-related events that were reviewed (out of 226) identified failure modes that are new and unique and not found in older analog systems, the remaining ~2000 records should be reviewed.

*For the purposes of this study, failure character is defined as the ensemble of failure modes that exhibit common characteristics.

4. REFERENCES

1. Energy Information Administration (EIA), Department of Energy (DOE). Accessed July 2009. *U.S. Nuclear Reactors*. http://www.eia.doe.gov/cneaf/nuclear/page/nuc_reactors/reactsum.html.
2. Energy Information Administration, Department of Energy. Accessed July 2009. *New Commercial Reactor Designs*. <http://www.eia.doe.gov/cneaf/nuclear/page/analysis/nucenviss2.html>.
3. U.S. DOE Nuclear Energy Research Advisory Committee and the Generation IV International Forum. December 2002. Accessed July 2009. *A Technology Roadmap for Generation IV Nuclear Energy Systems*. http://gif.inel.gov/roadmap/pdfs/gen_iv_roadmap.pdf.
4. L. A. Miller, J. E. Hayes, and S. M. Mirsky, *Guidelines for the Verification and Validation of Expert System Software and Conventional Software*, NUREG/CR-6316, SAIC-95/1028, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, D.C., March 1995.
5. J. H. Hayes, *Final Report for Fault-Based Analysis: Improving Independent Verification and Validation (IV&V) through Requirements Risk Reduction*, SAIC-NASA-98028, National Aeronautics and Space Administration, Fairmont, WV, December 2002.
6. J. H. Hayes, "Building a Requirement Fault Taxonomy: Experiences from a NASA Verification and Validation Research Project," *Proc. of the 14th IEEE International Symposium on Software Reliability Engineering (ISSRE'03)*, Denver, CO, November 2003.
7. J.-C. Laprie, *Dependable Computing and Fault Tolerance: Concepts and Terminology*, IFIP WG 104, LAAS Report No. 84.035, Kissimmee, FL, June 1984.
8. T. Saridakis and V. Issarny, "Towards Formal Reasoning on Failure Behaviors," *Proc. of the 2nd European Research Seminar on Advances in Distributed Systems (ERSADS'97)*, Valais, Switzerland, March 1997.
9. A. Sutcliffe and G. Rugg, "A Taxonomy of Error Types for Failure Analysis and Risk Assessment," *Int. J. Human-Computer Interaction*, **10**(4), pp. 381–405 (December 1998).
10. A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, *Basic Concepts and Taxonomy of Dependable and Secure Computing*, TR 2004-47, Institute for Systems Research, University of Maryland, College Park, MD (2004).
11. N. Siu, "Risk Assessment for Dynamic Systems: An Overview," *Reliability Engineering and System Safety*, **43**, pp. 43–73 (1994).
12. *Equipment Performance and Information Exchange System (EPIX): Reporting Requirements*, Institute of Nuclear Power Plant Operations, INPO 98-001, Revision 5.
13. Maintenance Rule reference.
14. NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants."
15. *Computer-Based Systems Important to Safety (COMPSIS) Project: 3 Years of Operation (2005-2007)*, NEA/CSNI/R(2008)13, September 2008, Nuclear Energy Agency.
16. Federal Aviation Administration (FAA). 2009. *Welcome to the Aviation Safety Analysis Information and Sharing (ASAIS) System*, <http://www.asias.faa.gov>.
17. *Offshore Reliability Data*. Accessed June 2009. www.oreda.com.
18. K. Korsah, M. D. Muhlheim, and D. E. Holcomb, "Industry Survey of Digital I&C Failures," ORNL/TM-2006/626, May 2007.
19. Westinghouse. *7300 System ASIC-Based Replacement Modules*. Accessed November 2009. February 2008. http://www.westinghousenuclear.com/Products_&_Services/docs/flysheets/NS-RRAS-0009.pdf.
20. N.G. Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, Reading, MA, 1995.
21. C. Garnet, and G. Apostolakis, "Context in the Risk Assessment of Digital Systems," *Risk Analysis*, **19**, 23-32, (1999).

22. T.L. Chu, unpublished private communication.
23. B. Li et al., "Integrating Software into PRA," *Proceedings of the 14th International Symposium on Software Reliability Engineering*, 2003.

APPENDIX A.

**TABULATION OF DIGITAL INSTRUMENTATION AND CONTROL
FAILURE EVENTS SELECTED FROM THE EPIX DATABASE**

APPENDIX A. TABULATION OF DIGITAL I&C FAILURE EVENTS SELECTED FROM THE EPIX DATABASE

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
1	Rod Block Monitor (RBM)	Programmable logic device (PLD) for RBM	NI	CPU lockup	RBM CPU lock up	NI	Personnel investigated RBM CPU lockup and discovered that the part number of the PLD (programmable logic control device) IC chip for the open drain IO card indicated a clock speed of 35 nanoseconds (ns), or 28.6 MHz for the open drain IO card. The proper clock speed should have been 55 ns, or 18.2 MHz. This incorrect clock speed can result in intermittent CPU resets due to noise on the data bus that can be misinterpreted by the processor. (Further investigation found that there had been several CPU resets since the system's installation.)	Incompatibility of hardware
2	Electrical Equipment A/C Unit (Class 1E)	Flow controller	Battery	Degradation of battery	Memory loss in digital controller	Loss of Essential Service Water (ESW) flow	Degradation of battery for the memory on the digital controller resulted in loss of programmed settings in controller.	Degradation/ age-related
3	High voltage distribution system	Static VAR Compensator (SVC)	Logic controller for SVC	Failure of subcomponent on controller logic circuit card	Shutdown of SVC	RAT failed to perform its function	Troubleshooting on the RAT SVC tracked the cause of the RAT SVC trip to the Thyristor Switched Capacitor (TSC) V1 branch controller logic circuit card. The card had failed to properly control the TSC V1. With the failed TSC V1 branch controller logic circuit card installed, the TSC V1 switched on unexpectedly providing capacitive reactive power when it was not required. The additional	Component failure

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							capacitive reactive power resulted in an unbalanced voltage. The phase voltage unbalance condition initiated the phase unbalance protective scheme and resulted in a RAT SVC trip. The apparent cause of the RAT SVC trip was a subcomponent failure of the TSC V1 branch controller logic circuit card. The RAT static VAR compensator system automatically shut down.	
4	Emergency electric power system [Emergency Diesel Generator]	Solid State Logic Module (SSLM)	Field programmable logic array (FPLA)	Loss of programmed logic	NI	Automatic closure of the 10A404-07 breaker in response to a loss of offsite power to the 10A404 bus and manual breaker closure from the Main Control Room would not have functioned due to this failure.	This solid-state logic module provides the interface between the Main Control Room bezel pushbuttons and status indications and the control relays for automatic and manual breaker operation. The observed failure cause was the failure of the field programmable logic array (FPLA) installed on the logic module. This was validated by bench test of the removed logic module and FPLA by I&C personnel. The solid-state logic module was validated to function properly; however, the FPLA installed on the module had lost its programmable logic. This failure did not inhibit the ability of the operator to manually close the D EDG output breaker locally at the 10A404 vital bus or from the 1DC422 remote generator control panel. Automatic closure of the 10A404-07 breaker in response to a loss of offsite power to	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							<p>the 10A404 bus and manual breaker closure from the Main Control Room would not have functioned due to this failure.</p> <p>The FPLA failure is identified as the causal factor of this event.</p>	
5	Turbine auxiliary cooling system (TACS)	Solid State Logic Module (SSLM)	Field programmable logic array (FPLA)	Loss of programmed logic	Incorrect output to control relay	TACS isolation valve failed closed.	TACS isolation valve failed closed due to failure of the non-safety-related SSLM. The SSLM provides the interface between the Main Control Room and the control relays for automatic and manual valve operation. The bench tests confirmed that the FPLA had lost its programmable logic, which resulted in de-energization of a normally energized control relay in the open control logic circuit, which closed the valve, isolated TACS flow.	Unknown
6	Anticipated Transient Without Scram (ATWS) System	Programmable Logic Controller (PLC)	Uninterruptable Power Supply (UPS)	Degradation of UPS battery	NI	None (plant was not in operation)	The ATWS UPS performs a self-test of internal components once per week, and as part of the test generates a momentary alarm. If the internal tests fail, the alarm will not clear. In this case, the self test detected degradation of the UPS battery.	Degradation/ age-related
7	Startup Transformer	Programmable logic controller (PLC)	Firmware (Software)	Incorrect firmware coding	Cycling of the PLC through the test mode	Voltage swings on startup transformer due to inability to	The firmware contains an internal <i>zero-crossing</i> sampling routine that would recheck the programmable unit by cycling through the test	Programming error OR Require-

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
						control voltage	mode. The incoming voltage may have had some switching noise, etc., that would cause the sine wave zero crossing to not match. *NOTE: new firmware version does not have this zero-crossing technique.	ments error/ misinterpreted requirements
8	Train A Balance-of-Plant Engineered Safety Features Actuation System (BOP-ESFAS)	Load sequencer	Programmable Peripheral Interface (PPI)	PPI Unresponsive/ lock up	Load sequencer failed to function	Only Train A, inoperable; other trains functional	Electrical noise caused the PPI to lock up, thereby incapacitating the load sequencer.	Operating Outside of Specifications
9	Stack radiation monitoring system (SRMS)	<ul style="list-style-type: none"> computer communication card ±5VDC power supply log count rate meter 	NI	Output degradation (due to static buildup)	NI Failure of communication card, power supply, and count rate meter.	Failure of SRMS to perform its function	Lightning strike caused static buildup and degradation until eventual failure of these three components: <ul style="list-style-type: none"> computer communication card ±5VDC power supply log count rate meter 	Operating Outside of Specifications
10	Turbine building radiation monitoring (TBRM)	Programmable logic controller (PLC)	PLC processor	NI	Loss of communication link	Failure to function	Failure of the PLC processor caused the communication link to go down. A software issue with the plant process computer also prevented a connection link with the plant stack monitoring system, whose PLC was operational.	NI
11	Radiation Monitoring System (RMS)	CPU Module	Octal bus transceiver (OBT) chip,	Failed output of address decoder chip	CPU Module locked up	Loss of communication with the RMS server	CPU module consisted of Intel 8085 CPU, four EPROMs for memory, timer/counters, programmable peripheral interface devices, an 8-bit	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
			EPROMs				<p>I/O port and proms for address decoding and bus buffering.</p> <p>Diagnostic monitoring of the radiation monitor determined that the microcomputer for the monitor failed.</p> <p>Octal Bus Transceiver (OBT) chip that performs address decoding and bus buffering in the microcomputer had failed.</p>	
12	Process Radiation Monitoring System	Microcontroller	Software	Software lockup	Out of service	No change of output indication w/ a change in input (failed as is)	<p>System Particulate Iodine and Noble Gas (SPING) of the Process Radiation System was discovered unresponsive to controls and indication. The SPING was returned to service by rebooting.</p> <p>Software lockup is an identified SPING failure mode. The condition is readily identified (unresponsive), rapidly corrected (power cycling) and occurs occasionally. Software lockup possibly due to interrupt queue overflow from abandoned channels.</p>	Programming error, OR Requirements error
13	Plant Management Information System	CPU (VAX 400-100)	Software	Faulty program calculation	Inaccurate Output	Incorrect Core Thermal Power (CTP) calculation	<p>During a routine check, it was identified that the comparison of turbine first stage pressure (impulse pressure) vs fraction of rated power (FRP) was unsatisfactory.</p> <p>Comparison of various inputs to the heat balance identified that there was a larger difference than normal</p>	Requirements error

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							for the plant conditions between % electrical generation and % CTP. Examination of shutdown and startup data for similar plant conditions indicated that the CTP calculation was in error. Operations identified that a change was made to the CTP calculation software to correct an error identified in the CNS Simulator. This error was to correct the modeling design in the simulator of the two-loop FW systems. This caused low CTP during single FW pump operation. A return to the prior revision of the CTP code will return the thermal power calculation to a verified and tested state.	
14	Toxic gas analyzer	Computer internal to the toxic gas analyzer	Software	Failure to communicate data to remote computer		Analyzer issued a system down error code that stated, "Cannot retrieve MODBUS gas data from database."	The analyzer's internal computer was not able to transport data to the remote (MCR) computer. Manufacturer stated that the error message, "Cannot retrieve MODBUS gas data..." indicated that the analyzer's internal computer was not able to copy the latest scan data and transmit it to the remote (MCR) computer. This should not have been a "system down" error, but a "requires service error," since the failure to transmit the data to the MCR would not prevent the analyzer from alarming when a true toxic gas event occurred. Manufacturer issued a new version of software to resolve "all	Programming error

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							outstanding software issues.”	
15	Feedwater System	Integrator/ Computation Module	Software	Unresponsive in auto mode	Startup Level Control (SULC) valve remained closed	Reactor Main Level Control (MLC) could not be placed in AUTO.	<p>During startup from cold shutdown, operator tried to put the SULC in auto mode; but the system did not respond.</p> <p>Simple troubleshooting was initiated and revealed the following: The AUT_MANLOGIC block for the Master Level Control (MLC) Panel Display Station (PDS) was in MANUAL and the set point had defaulted to 14 inches. This logic block resides in the main Digital Feedwater Control System (DFCS) computer, not the individual PDS. This switch of logic block mode would be transparent to the Main Control Room (MCR). When Operators placed the SULC control PDS in AUTO, the DFCS tried to maintain level at the control configurator set point of 14 inches instead of the 35 inches selected by the Operators at the MLC PDS. (This set point was a latent error from initial system installation in 1994).</p>	Incorrect interpretation of requirements

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
16	Condensate Polishing (CP) System	Pressure Differential Indicating Transmitter (PDIT)	Electronic Power Supply (24 V DC)	Voltage regulator card failed due to aging	PDIT output failed low	<ul style="list-style-type: none"> Unexpected closure of the CP Service Vessel Outlet Valves, Failure of the CP System Bypass Valve to open with a high Condensate System differential pressure (D/P) 	Event investigation revealed that Power Supply #1 in the CP Control Panel failed causing Pressure Differential Indicating Transmitter (PDIT) 5701 output to fail low. This pressure transmitter provides an input function to two alarms for system D/P, as well as an open permissive for the CP Bypass Valve CD-MOV-0132.	Degradation/ age-related
17	Steam Generator Blowdown and Wet Layup (WLU) System	PLC Module [Steam Generator Blowdown]	Electronic Power Supply	Open fuse (Voltage spike blew up the fuse)	Failure of flow control	All three S/G Drain/WLU Pumps failed	The SGBD WLU PLC power supply experienced an automatic shutdown. Per the vendor manual, this can be caused by the power supply sensing overvoltage, overcurrent, or undercurrent conditions at the output. The power supply also monitors incoming AC for proper levels. Any of these conditions can cause the power supply to shut itself down, for protection.	Operating outside of specifications

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
18	Steam Generator Blowdown (SGBD) and Wet Layup (WLU) System	PLC Module [Steam Generator Blowdown]	Electronic Power Supply	NI	Failure of flow control	S/G Blowdown alarm received	<p>Personnel investigating a “SGBD Alarm” noted that there were no alarms present on the SGBD/WLU control panel. A local check of the SGBD valves showed that all of the valves were closed. Check of the PLC showed that the DC power light was illuminated, but the “RUN” light was not. Further troubleshooting determined that the (PLC) internal power supply had failed.</p> <p>Likely cause was identified as degradation due to aging.</p>	Degradation/age-related
19	4.16 kV Electric Distribution System	Trip control for breakers	Scanner receiver card	Out of Tolerance (drifting) due to unstable clock	Breakers tripped	Distribution system out of service	<p>Unstable clock caused the clock frequency to be out of tolerance. When the clock frequency is out of tolerance, the card did not correctly process incoming signals. Attempts were made to adjust the clock frequency and stabilize it, but it did not work.</p> <p>* Failure is considered to be aging related.</p>	Degradation/age-related
		Motor-operated valve (MOV) controller	Scanner receiver card	Short Circuit	Closure of MOV		<p>Card had point 2 selected continuously, even if the point was not being selected by the logic. The circuitry was incorrectly continuously powering point 2. Attempts were made to recover the correct operation of this point; but it did not work.</p>	Degradation/age-related

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							Failure is considered to be aging related.	
20	Main Turbine Generator System	Main Steam Turbine. Electronic Pressure Regulator (EPR)	Analog output module	Erratic/fluctuating	Erratic/fluctuating output of EPR	Unable to regulate reactor pressure	The EPR was noticed to be failing downscale erratically and the manual pressure regulator (MPR) took control of reactor pressure, which was reduced with the MPR to the pre-transient level.	Unknown
21	Circulating Water System (CWS)	PLC (Circulating Water Hydraulic Intake Gate Flow Control Module)	NI	Unable to reset.	Gate remains fully closed.	CWS operated in closed cycle.	The hydraulic control system for the intake gates was unable to be reset. The pumps were repowered and capable of opening the gates but the CPU would not reset to allow correct positioning, control, or indication. The gates are fully closed, the light indications on the control room panel are not lit, and the indicator needles are downscale below the zero point. The PLC will not reset to allow gate movement. Plant remains in closed cycle due to inability to open gates.	Unknown
22	Condensate System Demineralizers	PLC	NI	“relay race” condition in PLC	PLC inoperable	Condensate system demineralizer inoperable.	Operations took condensate demineralizer off line to backwash and precoat per chemistry’s direction. However, backwash did not start when CYCLE START push button was pressed. With operations permission, the manual start was	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							<p>taken to Step 1 by a technician. This moves the PLC software program to Step 1. Then the technician took the manual start to Step 2. The display was checked and the system was working properly.</p> <p>The “relay race” causes the very first step to be out of sequence, and subsequently, the machine does not where it should be. (NOTE: The entry in EPIX defines this as the “relay race.”)</p>	
23	Refuel Platform Trolley	PLC	Software	Encoder Output Error	Spurious Motion	Trolley moved in the opposite direction	<p>The Refuel Platform trolley moved in the wrong direction while the Refuel Platform was moving toward a core bundle location. The move was being made in the automatic mode. During the move, the bridge was moving at the extreme north end of the core. It should have moved east to the required core location but it moved west. The safety travel interlock zone was entered and the bridge/trolley was stopped. Safety travel override was used to move away from the northwest corner of the core/vessel and the move was completed in manual.</p>	Programming error

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
24	Fuel Handling System (Refueling Platform Fuel Hoist)	PLC	Software	False Output	Loss of "Hoist Loaded" indication	Loss of "Hoist Loaded" indication	<p>The existing PLC design and computer system were not adequate to prevent the loss of "hoist loaded" indication considering the various dynamic conditions associated with movement.</p> <p>Numerous adjustments to the hoist drive as well as a load cell calibration were performed to resolve the problem. While these efforts improved the situation, the loss of "hoist loaded" indication occurred approximately 25–30 times during the re-channeling outage.</p>	Requirements error OR Incorrect interpretation of requirements
25	Blackout Diesel System (BDS)	PLC Module	Communication card	Communication Dropout	PLC Malfunction Alarm	BDS Unavailable	<p>Investigation of a "PLC Malfunction Alarm" determined that the latter was caused by loss of communication between the PLC and its remote I/O located in the cable spreading room.</p> <p>In contacting the vendor it was determined that a loss of communication can occur from failure of fiber or by accruing a certain amount of momentary losses or timeouts of communication, which lead to a dropout of all communication. The PLC assumes that the high number of timeouts mean no connection currently exists between the remote and local I/O.</p>	Maximum accrued timeouts
26	Blackout Diesel	PLC Module	Communication	Communication	PLC Malfunction	BDS Unavailable	The communications modem had	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
	System (BDS)		card	Dropout	Alarm		communications failure. The modem was rebooted with proper indication verifying that communication was established. The modem in the cable spreading room cabinet was verified to be communicating properly. During the time between the annunciator activating and clearing, the Diesel was unavailable.	
27	Blackout Diesel System (BDS)	PLC Module	Communication card	Communication Dropout	PLC Malfunction Alarm	BDS Unavailable	<p>It was previously determined that a loss of communication can occur by accruing a certain amount of momentary losses or communication timeouts leading to a dropout of all communication. The PLC then assumes that the high number of timeouts mean no connection currently exists between the remote and local I/O.</p> <p>It was concluded that the communication modems needed to be rebooted periodically in order to clear the timeouts from the memory.</p>	Maximum accrued timeouts

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
28	4.16 kV AC Electrical System	PLC Module	Processor board	Incorrect functioning of CPU or clock	PLC failed	<p><u>ALARMS:</u></p> <ul style="list-style-type: none"> • Bus Load Sequencer Trouble • Bus Load Sequencer Not In-Service <p>Bus Load Sequencer Inoperable</p>	<p>Control Room Annunciators “Bus 26 Load Sequencer Trouble” and “Bus 26 Load Sequencer Not In-Service” were received. Upon investigation, it was found that the Bus 26 Load Sequencer “Power On” and “DC Power” lights were not lit. The Bus 26 Load Sequencer was declared inoperable.</p> <p><u>Check for Common Cause and/or Generic Causes of the Failure:</u> All Safeguards Bus Load Sequencers are susceptible to this type of failure, since each Load Sequencer utilizes the same PLC model. The most likely cause of the failure was identified to be age-related degradation.</p>	Degradation/ age-relate
29	4.16 kV AC Electrical System	PLC Module	DC Power Supply and DC Undervoltage Monitor	Loss of DC power	Load sequencer inoperable.		<p>The control room received unexpected annunciator BUS 16 SEQUENCER IN TROUBLE. Operations responded per the applicable ARP and found the local PLC light not flashing and DC power supply light not lit. The Bus 16 Load Sequencer was declared inoperable.</p> <p>The failure was attributed to aging.</p>	Degradation/ age-related

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
30	Engineered Safety Features Actuation System (ESFAS)	PLC. (ESFAS auxiliary/emergency feedwater actuation common logic).	NI	Failed Output (high or low)	Modicon light was off	Trip alarm	Operations received a DAFAS B trip alarm. Alarm was determined to be invalid. A reset was attempted, but the trip alarm on the DAFAS panel did not clear.	Unknown
31	Station Blackout Gas Turbine Generator (GTG) System	PLC Module	Communication card	Loss of communication	PLC was reset; COMM light on PLC started to blink ON and OFF, which is an indication that PLC DH+ communications link malfunctioned.	GTG out of service	Gas Turbine Generator (GTG) operator found that the GTG #1 Human Machine Interface (HMI) display was not displaying the correct data. Symbols were found in place of the numbers that normally indicate GTG status. The Control Room was notified that GTG #1 was "Out Of Service". It was suspected that the Gas Turbine Programmable Logic Controller (PLC) had malfunctioned. Investigation showed that the PLC communications link had malfunctioned; the PLC was not communicating with external components.	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
32	Station Blackout Gas Turbine Generator (GTG) System	PLC Module	NI	Open breaker	False output	GTG Output Breaker opened automatically	<p>During the GTG Isochronous Test, the GTG #1 output breaker opened automatically. GTG #1 was near the end of the evolution of transferring the Unit 2 load to the EDG. The transfer happened at a fast rate; and the GTG output breaker tripped.</p> <p>Root Cause: The most probable cause for the breaker opening is that the PLC opened the breaker after analyzing the rapid load transfer from the GTG to the EDG when the Unit Operator manually increased the load on the EDG at a high rate of speed.</p>	Human error
33	Station Blackout Gas Turbine Generator (GTG) System	PLC Module	NI	Erratic Output	NI	GTG showed excessive load swings	<p>During a periodic load test, Gas Turbine Generator (GTG) #2 began to oscillate while paralleled to offsite power (DROOP mode of operation). GTG #2 was loaded to approximately 3300 kW, on its way up to 3600 kW when the oscillations began. The oscillations continued as the operator unloaded the GTG. When the generator output breaker was opened the oscillations ceased.</p>	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
34	Nuclear Steam Supply System (NSSS)	Control Element Assembly (CEA) Drive Mechanism	Optical isolation board (Component: Optical isolation chip)	Failure of CEA 48 to move specified distance on command.	CEA misalignment from its subgroup	Four Core Protection Calculators (CPC) generated a reactor trip on low DNBR	<p>Plant automatically scrammed from approximately 64 percent reactor power as the unit was being shut down. All protective systems operated as designed. The core protection calculators (CPCs) tripped the reactor on low DNBR. During the CEA movement, CEA 48 had not moved below 147.0 inches withdrawn. As a result, a CEA deviation caused a large penalty factor to be transmitted to the CPCs. The CPCs responded appropriately from a possible localized high power condition. The deviation alarm from the CEA calculator actuated seconds before the trip.</p> <p><u>Notes:</u></p> <ul style="list-style-type: none"> No alarm was provided, nor was instrumentation readily available to detect and warn operators of CEA deviation at the top of the core. No engineered safety feature actuations occurred during the event and none were required. 	Degradation/age-related
35	Plant Multiplexer System (PMUX)— <i>Site Common Name: Remote Multiplexer Terminal (RMT)</i>	CPU Module	Circuit board/card (I/O Card)	Loss of Communication/ Common bus failure	Failed to communicate	RMT ceased communication with the loop; the Ethernet network card appeared to have failed to communicate with the CPU	<p>PMUX controls the cooling tower fans, which directly affect the Unit's power output. Unit was down-powered to 92.5%. Cooling towers also had water overspill issue.</p> <p>The I/O card output changed state to a "0" output. The post-incident</p>	Corrosion

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
						module	<p>inspections revealed that CPU module appeared to be undamaged and passed all the manufacturing tests. The same RMT failed again which caused another loss of Cooling Tower #1 indications but no inadvertent fan de-actuations.</p> <p><u>Root Cause:</u> Water introduction into the instrument cabinet was the contributing cause of the system backplane corrosion, which affected the common bus that feeds the system modules.</p>	
36	Operator Aid Computer (OAC); Digital Control Rod Drive Control System (DCRDCS)	DCRDCS Network Switch	NI	DCRDS network switch disconnected.	Loss of communication between OAC and DCRDCS	NI	<p>Cause is believed to be the power perturbation related to the DCRDCS Network Switch.</p> <p>The failure of the OAC interface with the DCRDCS resulted from loss of communications between the DCRDCS OPC Server and the DCRDCS PLCs. The data analysis showed that the DCRDCS Network Switch lost power and restarted. When this occurred, the DCRDCS OPC Server indicated a failure of the connection. This loss of communications resulted in failure of the ICS Triplex—Trusted OPC Server Application and subsequent loss of communication between the OAC and the DCRDCS.</p>	Loss of power

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
37	Control Rod Drive (CRD) System; Liquid Standby Control (LSC) System	CRD OPC Server and Operator Aid Computer (OAC) OPC Gateway	NI	Loss of Communication	Communication failure between the I/O server and PLC	Loss of Standby Liquid Control (SLC) monitoring	Unit 3 experienced a loss of SLC monitoring due to communication failure between the CRD OPC Server and the OAC OPC Gateway.	Unknown
38	Essential Siphon Vacuum (ESV) System; Siphon Seal Water (SSW) System	Operator Aid Computer (OAC); Data Management & Communications System (DMACS) Gateway	Software	Loss of Communication	Interface communications between the OAC and the DMACS Gateway failed.	ESV System and SSW System in Units 1, 2, and 3 received numerous alarms on OAC.	Intellution Fix32 (an application on the Gateway) interface handles communication between the OAC and the PMC; and the OAC and the ESV/SSW PLCs. The DMACS gateway was rebooted and the Unit 2 system returned to normal.	Unknown
39	Fuel Handling (FH) and Transfer System	PLC	Software	Pump failure (mode of failure not indicated)	Inherent fault in PLC logic revealed during diagnostics	Fuel shuffling procedure delayed; Fuel Handling and Transfer System operated, but not within specified parameters.	The event was caused by a failure of a Sundstrand Corp Model LMV pump. Troubleshooting of the power failures for the F15 Fuel Handling (FH) bridge revealed a deficiency with the PLC logic in capturing fault data. Wiring/software deficiencies identified during troubleshooting caused significant challenges to the troubleshooting team that ultimately delayed identifying and repairing the cause of the FH bridge power failures and resulted in a 10 hour slip in critical path time and unnecessary replacement of parts.	NI

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
40	Radioactive Gaseous Monitoring System (RAGEMS)	PLC	NI	Loss of communication (PLC)	Communication failure with Plant Process Computer (PPC).	PPC cannot provide required inputs to the Safety Parameter System Display (SPSD).	The Turbine RAGEMS Mini Programmable Logic Controller (Mini PLC) failed, thus interrupting communications of the RAGEMS data to the Plant Process Computer (PPC).	Unknown
41	Radioactive Gaseous Monitoring System (RAGEMS)	PLC	NI	Loss of communication (PLC)	PLC failure	Turbine RAGEMS was declared inoperable.	The problem occurred due to the failure of the Programmable Logic Controller (PLC) for the Turbine Building RAGEMS, which in turn caused the Turbine Building RAGEMS link to go down.	Failure of PLC for the turbine building RAGEMS
		Plant Process Computer (PPC)	Software		PPC software required that link to both PLCs be alive.	Generated alarm " <i>Stack/Turbine Building RAGEMS Trouble</i> "	Restart of RAGEMS Link task showed another issue as the RAGEMS link task will not connect to Stack Building RAGEMS whose PLC was operational. This problem was caused by a software issue with the new Plant Process Computer (PPC).	Requirements error/ incomplete requirements description OR Misinterpreted Requirement
42	Gaseous Effluent Monitoring System (GEMS)	PLC Module	Communication card	Loss of communication	Failed to communicate	Loss of communication between the Main Stack Monitor and the GEMS computer	Stack and Vent GEMS was declared inoperable due to loss of communication signals from the GEMS computer system. Investigation of this event could not determine any conclusive causes why the computer communication card failure, the ± 5 VDC power supply trip, and the log count rate	Operating outside of specifications

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							<p>meter malfunction occurred at the same time. The most probable cause appears to be that the Stack GEMS experienced static buildup or voltage transients caused by an electrical storm that occurred 17 hr prior to the event.</p> <p>It was found that the Computer communication card does have a history of failing when the room temperature is above 80°F.</p>	
43	Engineered Safety Features Actuation System (ESFAS)	Diverse Auxiliary/Emergency Feedwater Actuation System (DAFAS) Actuation Logic	Fiber Optic Modem (FOM)	NI	DAFAS Channel B declared inoperable; both DAFAS channels A and B bypassed	NI	<p>DAFAS channels A and B were placed on BYPASS due to frequent receipt of spurious alarms.</p> <p>Operations informed that they received an alarm with no error message; but most of the time the error is for PLC 1 with no indication why the error was received.</p> <p>The FOM supplier has gone out of business; modem and supporting unit designs had to be changed.</p> <p>*The failure is reported to have resulted from random electrical/ electronic component failure</p>	Electronic component failure

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
44	Core Protection Calculator System	CPU Module	CPU motherboard	CEA deviation, sensor failure (mode of failure not indicated).	NI	<u>ALARMS:</u> <ul style="list-style-type: none"> Control Element Assembly Calculator (CEAC) sensor failure CEAC CEA deviation 	Unit 2 control room received various failure alarms: Sensor failure, CEA Deviation, and Channel Sensor Failure. CPC trouble lights were lit on all four CPCs, and CEAC trouble light on 'C' CPC.	Unknown
45	Radioactive Gaseous Effluent Monitoring System (RAGEMS)		Internal Power Supply	NI	PLC failed	RAGEM system cycled on and off.	While performing the quarterly Tech Spec Surveillance Test on the Noble Gas Normal Range Monitor, the grab sample light on the system control board (local panel) did not light on the alert signal, nor did the system obtain a grab sample as designed... The cause of the failure of Remote Programmable Controller for Radioactive Gaseous Effluent Monitoring System (RGEMS) was failure of an internal power supply. The power supply failure caused the RAGEM system to cycle on and off.	NI
46	Instrument and Service Air System	Local Control Board (Touchpad on Air Compressors)	Erasable Programmable Read Only Memory (EPROM)	Instrument air pressure drop	Spurious commands generated	Loss of instrument air	<p>The plant entered into Loss of Instrument Air due to Instrument Air Compressor unloading while in-service causing instrument air pressure to drop and resulting in the automatic start of Instrument Air Compressors.</p> <p>It was previously identified that there was a potential problem with the local control touch pad. The</p>	<p>Programming error</p> <p>[Embedded (software) problem with the version of firmware (EPROM chip) currently in</p>

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							<p>problem could result in spurious or unwanted commands while pushing the Display button or other areas on the touch pad.</p> <p>The vendor of the controller recommended that an EPROM chip on the control board be replaced with an updated version.</p>	use with the module]
47	Radiation Monitoring and Sampling System	PLC	NI	NI	Lock up or CPU failure to complete a routine.	Isolation valves were shut, which prevented the flow through the normal and accident range filters	The control room was informed that particulate and iodine filters were found isolated. Operations and I&C Maintenance could not identify any scenarios that could have led to the situation. It appears that the logic controller failed causing all the isolation valves to shut which prevented the flow through the Normal and Accident range filters.	NI
48	Plant Computer System	CPU	Software Task	Task crash [Loss of asynchronous system traps (AST) ^a]		Failover to backup computer	<p>A particular task designated "critical" ran out of allocated ASTs initially assigned by the configuration. When the task had no more AST's available, it is unable to open new files or read/write to existing ones.</p> <p>As an immediate measure, the task was designated as non-critical until the issue with the task is fully addressed.</p>	Programming error OR Incomplete requirements specifications.

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
49	Control Rod Drive System (CRDS)	CPU Module [Rod Worth Minimizer (RWM)]	Output Buffer card (Electrolytic capacitor on the circuit board in the output buffer)	Electrolytic capacitor failure (Actual mode of failure not specified)	RWM failed diagnostic test.	No direct effect on the system; no change in core reactivity or reduction in reactivity control	Self-diagnostic portion of the RWM surveillance initially failed. Troubleshooting showed that during the diagnostic mode, the Select Block permissive was failing to reset. This is what was causing the RWM diagnostic test to fail... Further testing determined that a capacitor on the RWM Output Buffer circuit board had failed. Replacement corrected the problem.	Age-related
50	Safety Parameter Display System (SPDS)	SPDS Archive Server	Software	Application crash	Server Network Manager application crashed Dr Watson (a Microsoft utility) gave a warning message that required user interaction, which prevented the fail-over to the backup server	Disconnection of SPDS from two SPDS PCs in the control room and Work Support Center PC	Dr. Watson (a Microsoft utility) error dialog requires an operator to acknowledge the error. Therefore the crash of the server application was not notified to the operating system.	Unknown (Lack of operator acknowledgment was not the cause of the server application error)

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
51	Process Computer Equipment System [Site common name: Emergency and Plant Information Computer (EPIC)]	Host computer	Software	Erratic/unstable output	NI	EPIC was found to auto-swap from narrow- to wide-range level transmitters at about half the preprogrammed value	<p>The SPWL algorithm in EPIC was found to auto-swap from narrow to wide range level transmitters at about half the pre-programmed value of 0.08 feet written in software file SPWL.FOR and required by the SPDS Design Manual.</p> <p>The problem was eventually traced to an incorrect version of the SPWL algorithm that was placed in the EPIC Object Library without any authorizing plant design change, and which remained quiescent until the day after a software design change necessitated a recompilation.</p>	Inadequate software version control
52	Plant Process Computer (PPC) System	PPC	Software (Shift Average Program)	Computer screen not updated.	Unit 2 PPC shift average program was not updating the Unit 2 PPC screen	NI	PPC software bug; the Unit 2 PPC shift average program was not updating the PPC screen. (NOTE: documentation on this event was sparse; there was possibly an application crash which manifested itself as a frozen screen).	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
53	Process Radiation Monitoring System	CPU Module [Effluent Radiation Monitor Control]	Software	Communication lockout due to accumulation of timeout errors	Module was declared inoperable.	Radiation monitoring system inoperable.	Eberline Radiation Monitor unit was rebooted three times. Vendor software programmers identified flaws in the programming that caused communication link timeout errors to accumulate in the buffer until a lockout occurs. Some evidence also suggested that EMI disturbances affected communication links and exacerbated the problem.	Programming error and/or Operating outside specifications
54	Feedwater Pump Turbine Controls System	CPU Module [Low-Pressure Servo Drive Interface (LPSDIF)]	Actuator Interface Card	Component failure (actual failure mode not indicated)	NI	Feedwater pump failed to control in "Manual" or "Automatic" modes.	The failure in the feedpump controls, which prevented the feedwater pump from controlling in Manual and Automatic modes, was due to an internal failure in the Low Pressure Servo Drive Interface (LPSDIF) module.	Unknown
55	Reactor Coolant System (RCS)	In-core Temperature Monitor Recorders	Software	Unscheduled clock reset. (Communication interruption as a result lasted 36 seconds)		NI	Failure was first thought to be the result of battery failure. However, a battery failure would give an error message on the recorder and no AC power interruption was noted. The cause of the clock reset is considered to be memory corruption performed by the recorder's software. Investigation also revealed that another result of this event was that temperature data from the recorder to the SPDS were interrupted for 36 seconds.	Memory corruption of recorder software

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
56	Reactor Recirculation System	Recirculation Pump Variable Frequency Drive (VFD) Control Module	NI	VFD controls failed (mode of failure not indicated)	VFD controls failed	Recirculation system unavailable; reactor was scrambled manually!	VFD controls failed due to excessive traffic	Excessive traffic (interference or data storm) on the connected plant network
57	Reactor Water Cleanup (RWCU) System	PLC	Power supply; output cards; capacitors	Damaged capacitors (mode of failure not indicated)	PLC did not work	Loss of RWCU flow	Failure of a PLC caused closure of filter demineralizer flow control valves, resulting in a low-flow pump trip.	Degradation/ age-related
58	Reactor Water Cleanup (RWCU) System	PLC	Power supply, controller, output cards	Damaged components on output cards (actual failure mode not indicated)	Power supply failed; output cards had a damaged component	Loss of RWCU flow	Initial troubleshooting found that the power supply had failed. Further investigation revealed that one of the output cards had a damaged component. PLC power supply, controller unit and three output cards were replaced. It was observed during the repair that material condition of all circuit cards was degraded; slight corrosion on some connections, discoloration of electronic devices were all attributed to long term use and aging.	Degradation/ age-related
59	Reactor Water Cleanup (RWCU) System	PLC	Power supply	NI	NI	Loss of RWCU flow	RWCU PLC has experienced five failures over a four-month period. The contributing cause was found to be age-related degradation or failure (20+ years of service).	Degradation/ age-related

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
60	Reactor Water Cleanup (RWCU) System	PLC	Power supply	NI	NI	Loss of RWCU flow; pump trip	RWCU PLC has experienced five failures over a four-month period. The contributing cause was found to be age-related degradation or failure (20+ years of service).	Degradation/age-related
61	Reactor Water Cleanup (RWCU) System	PLC	Power supply	NI	NI	Loss of RWCU flow; pump trip	RWCU PLC has experienced five failures over a four-month period. The contributing cause was found to be age-related degradation or failure (20+ years of service).	Degradation/age-related
62	4.16-kV System Class 1E Transformer	PLC	NI	PLC failure (Mode of failure not indicated)	Capacitor bank failed to perform the designated "FREEZE" function.	NI	While performing a check, Loading Diesel Generator computer point did not indicate FREEZE. This indicated the failure of the capacitor bank NB03 to freeze. That is, the capacitor bank could not respond to the input requesting the capacitor bank to freeze from turning on the capacitor banks. This was traced to a problem with the PLC in NB03. (NOTE: During troubleshooting, the PLC was reset and at that time, the freeze function locked in (i.e., latched). At this point the capacitor bank could no longer perform its intended functions to "...maintain the preferred source in the event of changing switchyard voltage").	NI

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
63	Radiation Monitoring System	CPU Module	NI	Computer lockup	CPU module did not function	Communication line failure; radiation monitor computer lockup	Control room received a "COMM LINE" failure; and annunciator "RAD MON COMPUTER LOCKUP" alarmed. Reported as random failure.	Unknown
64	Radiation Monitoring System	CPU Module (Intel 80/24A CPU board)	Universal Synchronous/ Asynchronous Receiver/ Transmitter (U37)	Computer lockup	Loss of communication with the Remote Indication and Control (RIC) unit in the control room	Communication line failure; radiation monitor computer lockup	Control room received a "COMM LINE" failure; and annunciator "RAD MON COMPUTER LOCKUP" alarmed. *Reported to be a random failure.	Unknown
65	Isolation Condenser (IC) System	Make-up Pump PLC	NI	PLC failed to reboot	PLC failed to reboot	The LCD display was backlit with no display; the pump status light was off; there was no control room indication; and the trouble alarm failed to annunciate for low (water) temperature.	An isolation condenser make-up pump PLC failed to reboot upon Remote Trip Signal (RTS). Failure reported to have occurred multiple times.	Unknown
66	Reactor Building Storage Pools System	PLC	Software (Hoist Loaded Subroutine)	Incorrect PLC output	NI	A "Hoist Loaded" condition (light) is required to be energized when weight on the grapple is less than or equal to 535 lbs. The "Hoist Loaded"	In preparation for pre-outage irradiated fuel movement procedures, it was determined that one of the acceptance criteria could not be met. The purpose of the Hoist Loaded PLC is to provide input to the refueling interlocks that fuel is loaded on the grapple and that no control rods can be withdrawn when	Inadequate software V&V

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
						light came on when weight on the hook was approximately 548 lbs.	<p>the refuel bridge is over the core. The Hoist Loaded PLC was also supposed to discriminate between a fuel bundle versus a double blade guide (DBG). Problems with the PLC code resulted in failure to meet the requirements.</p> <p>PLC setpoint was determined to be less conservative than required by the Technical Requirements Manual</p>	
67	Fuel and Reloads System; Load Weighting System	PLC	Network interface card	Failed to establish communication	Screen was blank and an attempt to restore the unit was unsuccessful. Power had to be cycled.	<p>A system fault alarm condition was received on the operator interface computer.</p>	<p>The current network interface card on the PLC had a default nodal address of 69. It was identified that the card was failing to its default value.</p> <p>Later, it was identified that grapple solenoid was missing a surge suppressor, though shown on the elementary drawing.</p> <p>It's concluded that a voltage spike on the power supply caused the failure of the PLC.</p> <p>This is considered a Design Configuration failure for (1) using a common 115 VDC source for operation of the grapple solenoid and the PLC, (2) not installing the surge protector as per the original drawing supplied by the vendor.</p>	Installation error; also Operating outside of specifications

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
68	Condensate/ Feedwater System; Condensate Demineralizer Controller	PLC	Software	Erroneous/False Output	PLC switched each of the 7 demineralizers to manual control with 0% flow demand, which resulted in trip of both reactor feedwater pumps (RFPs).	Automatic reactor scram on low reactor water level. Following the scram, reactor water level (RWL) continued to decrease due to void collapse, which resulted in closure of Containment Isolation Valves. Eventually, Reactor Core Isolation Cooling (RCIC) and High Pressure Coolant Injection (HPCI) systems initiated automatically and recovered RWL.	An engineer was installing software on the Chemistry Data Acquisition System (CDAS) server from the business LAN to conduct a test to verify connectivity to the CDAS server and transmit condensate demineralizer values. The Condensate Demineralizer PC was connected to the network and the test was conducted. However, during the test, the Wonderware Suitelink communication path synchronized the data tags from the CDAS server Wonderware through the firewall to the production Condensate Demineralizer PC Wonderware system. Because the data tags on the test software installed on the CDAS server did not have actual operating parameters—but only zeros, the Condensate Demineralizer PLC tags were overwritten by zeros, which resulted in 0% flow demand and essentially complete isolation of condensate flow to the feedwater system. This caused initiation of Reactor Core Isolation Cooling (RCIC) and High-Pressure Coolant Injection (HPCI) systems to recover reactor water level (RWL).	Human error (Application parameters were inadvertently updated (all reset to 0) when software was installed during a test.)

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
69	Plant Process Computer System	Process Computer	A/D Converter	“Open circuit/loss of continuity”	Loss of process computer (failure to communicate)	No data available on digital displays, the NSO’s CRT’s, alarm or demand CRT’s, Powerplex and Safety Parameter Display System (SPDS) display	Control room operators observed a loss of the station process computer. No data available on digital displays, the NSO’s CRT’s, alarm or demand CRT’s, Powerplex and SPDS display.	“Open circuit/loss of continuity” is given as the general/specific cause.
70	Emergency Response Facility/ Emergency Response Data Acquisition and Display System (ERF/ ERDADS) System	CPU	Circuit board/CPU board	Periodic processor hang-up	Processors hung up	ERDADS became inoperable	Computer cabinets were covered with protective blankets during welding activities in the overhead, which caused temperature rise in the cabinets. Processor boards became abnormally temperature sensitive. Computers run with cabinet doors open, but closing cabinet doors forces a computer lockup after 24 to 36 hours. Processor hang-up caused an attempted automatic failover in one train. However, the other train did not assume master status when requested. A reboot was required to correct it.	Inadequate environmental control
71	Containment Atmosphere Radiation Monitoring System	Control Room Display, Control for the Radiation Monitor	8-volt power supply	Erratic Output	NI	Loss of monitor indication in control room	Control room display/control for the Unit 3 containment radiation monitor experienced erratic display indications due to an internal 8-volt power supply failure.	Power supply failure

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
72	Containment Atmosphere Radiation Monitoring System	Control Room Display, Control for the Radiation Monitor	8-volt power supply	Erratic Output	NI	Loss of monitor indication in control room	Control room display/control for the Unit 4 containment radiation monitor experienced erratic display indications due to an internal 8-volt power supply failure.	Power supply failure
73	Drywell Cooling System	CPU	Circuit board/CPU board	Spurious performance (CPU board)	NI	Drywell chiller tripped.	Drywell Chiller tripped due to a detected signal greater than 10%-rated load. The microprocessor board was checked at the time of the trip and no problem was found; however the board was replaced as a preventative measure. The cause of the trip appears to be the EMI interference on the microprocessor cables. It was found out that welding began in the Diesel Generator Building. The welding machine was connected to the ground that is ultimately connected to the piping. The ground potential was observed with an oscilloscope; when welding is finished, the high-amplitude, high-frequency waveform disappeared.	Operating outside of specifications
74	Reactor Protection System [Solid State Protection System (SSPS)]	Manual/Automatic Reactor Scram/Trip Common Logic	SSPS Isolator Board	Spurious performance (isolator card)	NI	Spurious alarms and computer point indications	Spurious alarms were received for about six months. The isolator card was replaced, and no alarms were observed thereafter.	Degradation/ age-related

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
75	Standby Gas Treatment System (SGTS)	Instrument Controller	Battery	Loss of memory	Generated trip signal	The SGTS Train Heater was sent a TRIP signal that prevented it from	The controller lost its programming and became inoperable.	Battery failure
76	Emergency Diesel Generator (EDG) System	Solid State Logic Module (SSLM)	Field Programmable Logic Array (FPLA)	FPLA failed (mode of failure not indicated)	SSLM did not perform its function	Loss of breaker status indication (in control room).	During a console walkdown, the status indication bezel for the 4-kV EDG output breaker was not illuminated, i.e., loss of breaker status indication, resulting in unplanned inoperability of one of the EDG's. The I&C personnel found out that this was caused by a failed logic module (SSLM). The SSLM provides the interface between the Main Control Room bezel pushbuttons and status indications, and the control relays for automatic and manual breaker operation. Further investigation of the module revealed that an FPLA on the SSLM was the failed component.	Unknown
77	Turbine Heater Drains System	Level Tracking Driver (NTD)	Current Output Circuit (Integrated Circuit), and a transistor	NTD card output failed high	NTD inoperable	Reheater (RHTR) Drain Tank and Normal Drain Tank valves failed to remain closed (drifted off closed seat)	Control room received Feedwater Heater (FWH) Hi Level Alarms. Operators also noted the RHTR Drain Tank and Normal Drain Valve were full open	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
78	HVAC System (Main Control Room (MCR) Chiller)	Logic Board	Relay Connector	Disengaged	NI	MCR chiller failed to maintain cooling in the main control room habitability zone	MCR chiller experienced a “Lost I/O” alarm and shutdown. Investigation revealed that during normal operation, the vibration of the chiller package caused the relay to loosen and back out about 1/4 inch and become disengaged with the digital board, therefore breaking the circuit and causing the chiller to trip. An administrative change was initiated to replace the output circuit boards with soldered relay connections	Degradation/ age-related (vibration)
79	Plant Computer System	Data Acquisition Processors (CPU Module, multiplexers) There are 6 multiplexers: A, B, C, D, E, F. In this case, MUX C failed.	NI	Loss of logical network connection from the computer to the MUX processor	MUX became unreachable”; even though the physical link appeared to be intact; the computer could not make a network connection to the MUX.	Partial loss of display of critical data points on Safety Parameter Display System (SPDS).	MUX C failure was due to loss of the logical network connection from the computer to the MUX processor. The MUX C supplies computer points used on the six SPDS critical safety function (CSF) trees. The computer correctly indicated the failure of each of the MUX C computer points. *The anticipated cause is that some undetermined computer system resource becomes “limited” after extended runs without computer restart.	Operating beyond limited software resources

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
80	Plant Process Computer System (PPCS)	Analog Input Gate Card (of one of the two MUX analog input chassis)	NI	NI (Failed analog input card)	Reference voltages varied between 50% to 10% of their expected value (see Description of Digital Event)	NI (other analog input chassis remained functional and interfaced normally with PPCS)	Unit 1 and Unit 2 received numerous PPCS alarms for the Yellow PPCS MUX power supplies, including +5, +48, +15 and -15V System Voltage alarms. The problem was isolated to one of the two Yellow MUX analog input chassis. Each PPCS MUX contains two analog and two digital input chassis. The problem was first thought to be related to the Analog-to-Digital (A/D) card in the failed chassis. Later it was identified that the failure was related to a failed analog input gate card. *All attempts to alter the scanning configuration of the failed chassis did not identify the faulty card, and only physical removal isolated the problem.	Unknown
81	Plant Process Computer System (PPCS)	Computational Server <ul style="list-style-type: none"> • Drop 129—primary • Drop 131—backup 	NI	Loss of communication (to the PPCS network)	Did not switch over to Drop 131	PPCS malfunction	PPCS drop 129, the primary computational server, lost its connection to the PPCS network. Drop 131, which was in backup, did not pick up as primary. Reactor Trip Override (RTO) indication and DT indication were lost. It was later found out that there was heavy FDDI (network architecture) traffic, which caused a parity error. There was an error on port 11 on drop 129 and was unable to communicate with drop 131 to tell it to become the primary.	Inadequate software V&V

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
82	Reactor and Safeguard Protection System; Engineered Safety Features Actuation System (ESFAS)—Train A	Solid State Protection System (SSPS) Logic Circuit [Universal Logic Board (ULB) for Main Steam Line (MSL) differential pressure (DP) Safety Injection (SI) actuation]	NAND gate (in Z9 chip)	NAND gate output failed in a quasi-trip state (would not provide a true "HI").	Failed ESFAS train A logic circuit.	A trip status indicating light, main control board alarm, and associated computer alarm actuated.	An annunciator, TSLB light, and computer point came into alarm indicating a 1B Steam Generator Steam Line High Delta P Alert. First, it was thought that the symptom was due to a failed channel. Troubleshooting determined that the failure was due to a failed ESFAS—Train A logic circuit. Initial bench testing of the Universal Logic Board (ULB) showed that the card's 2 of 3 logic circuit initiated a trip signal when either redundant channel was in a tripped state. Upon further investigation of this ULB card failure, it was found that a NAND gate in the logic circuit had failed in a quasi-trip state. The output of the failed NAND gate would not allow a true HI (>7.5 VDC). Although the NAND gate would not provide a true HI, it would provide a 7.0–7.2 VDC output. This degraded output was high enough for the failed ULB to place itself in a fail-safe condition. The Z8 chip being pulled low resulted in the annunciator, TSLB light, and computer alarm to actuate/illuminate.	Operating outside specification

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
83	Nuclear Instrumentation and Neutron Monitoring System	Gamma-metrics Indication at Hot-Shutdown Panel (HSP)—Display Driver Card	Power supply	NI (Display driver cards failures)	Loss of display	Loss of Gammametrics indication at HSP; Main Control Board still maintained the proper indication.	It was noted that the GammaMetrics indication at HSP had been lost. It was determined that excessive heat from the 250-VDC power supply caused failures of the display driver cards.	Operating outside specification
84	Reactor and Safeguard Protection (including Anticipated Transient Without Scram Mitigating System Actuation Circuitry—AMSAC) System	Universal Logic Board [Solid State Protection System (SSPS)]	NAND gate	NI	NI	Reactor trip	Unit 2 reactor tripped during low power physics testing from a B train Source Range Hi Flux signal. Both trains of source range trips had been blocked for approximately 10 minutes, when the B train source range block reset. Only the B reactor trip breaker opened. Reactor was tripped manually to open the A trip breaker.	Unknown
85	Safety Parameter Display System (SPDS)	CPU	Isolation transformers in the non-redundant peripheral switch	Processor hang up	NI	SPDS operator consoles were not updating in the Control Room (CR). Additionally, the two graphic display screens were unresponsive to operator commands.	Investigation revealed that the Unit 2 SPDS operator console in the Technical Support Center (TSC) was not updating. The Unit 1 Shift Engineers reset the “A” SPDS computer, which returned the SPDS to normal updating in the Unit 1 Control Room. However, the Operator Console would not respond to operator commands. Computer Support (CS) rebooted both A and B SPDS computers, which returned both computers to a fully functional status. CS personnel also performed troubleshooting of the Unit 2 TSC SPDS Computer. CS personnel	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
							verified that Unit 2 information could be supplied to the Unit 1 TSC SPDS Computer.	
86	Safety Parameter Display System (SPDS)	Control room console	Isolation transformer in non-redundant peripheral switch	NI	No display (Unit 2) or cryptic display (Unit 1) on console	SPDS remains operable; the Unit 2 data are available at the TSC using the Colorgraphics Module.	<p>During the performance of a Monthly Alternate Shutdown Channel Check, the three operating modules in the Technical Support Center (TSC) for Unit 2 had no display, and the Unit 1 modules were displaying unreadable (cryptic) values.</p> <p>It was found that SPDS isolation transformers in the non-redundant peripheral switch had failed rendering the U1 control room console out of service.</p>	Unknown
87	Safety Parameter Display System (SPDS)	SPDS operators console	Touchscreen (as an input device)	Unresponsive to input command	Operator console nonresponsive	SPDS touchscreen trend displays remained functional and were updating with valid data; however touchscreen input functions were not responsive to user commands.	SPDS operators console locked up and would not respond to any commands. It took several reboots to put the system in service. Once they were operational, the same failure repeated with no change with successive reboots.	Unknown

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
88	Engineered Safety Features Actuation System (ESFAS)	Trip Logic Module [Channel 6]	Rotary switch Relay internal to module	Loss of trip signal	Isolation and reactor building cooling channel did not generate the expected trip signal	Did not get a trip signal from Channel 6 upon pressure test switch in test position	During performance testing of Unit 1 ESFAS analog channel 3 test, the building pressure test switch was placed in test. No trip signal was generated by digital channel #6 (isolation and reactor building cooling trip). The failure was attributed to an intermittent failure of either the rotary switch or the affected relay internal to the module.	Intermittent failure of rotary switch or relay internal to module.
89	Safety Parameter Display System (SPDS)	CPU Module	NI	No output indication	NI	SPDS inoperable/unavailable	SPDS Train A failed in the Unit 1 and Unit 2 control rooms. During this failure, SPDS Train B was declared unavailable due to being aligned for a scheduled Emergency Plan Drill. This resulted in SPDS being totally unavailable. The Train A of the SPDS was successfully restarted in 10 minutes.	NI
90	Safety Parameter Display System (SPDS)	SPDS Console	NI	NI	NI	SPDS consoles not functional	The Emergency Operations Facility (EOF) SPDS consoles had been non-functional for at least 60 minutes. "B" SPDS was OOS to reduce heat loads on the SPDS computer room. The "A" SPDS was functioning in the control rooms; but the EOF consoles were not functional. Rebooting the consoles had no effect.	NI

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
91	Electro-hydraulic Control System in Main Feedwater Pump (MFP)	Control system signal processor board	+5V power supply (in Logic Channel A)	(Power supply) (actual failure mode indicated)	NI	MFP Turbine Control System Trouble Alarm received	The alarm was determined to be signal processor power supply problem. It was determined that the Logic Channel A +5V Power Supply for the A main feedwater pump had failed.	Unknown
92	Delta T and Tave loop for Reactor Coolant System (RCS)	7300 Processor support module (Integrator/Computation Module)	Lead/Lag Amplifier Card (NLL)	NI	Erratic Output (Core Delta T and Loop Tavg)	Alarm, indication in control room.	Control room received DeltaT Deviation Alarm and DeltaT Withdrawal BLK Alarm. Loop 1 DeltaT plant computer point spiked high due to a degraded ASIC and NLL card. Removed failed ASIC card with a new (ASIC) card and failed NLL card with a new NLL card.	NI
93	D Train steam pressure indication	7300 Processor support module Loop power supply and isolator card (NLP)	Capacitor on card	Shorted capacitor	Erratic Output on NLP card caused Steam Generator Pressure Transmitter to fail LO	The plant experienced a maximum of 0.16% increase per Delta T indications during the entire event.	Steam Generator steam outlet pressure transmitter failed low due to an intermittent failure of the NLP card. The analysis performed on the card concluded that a capacitor was shorted causing increased current in the circuit and blowing a fuse. The NLP card was replaced with an ASIC counterpart.	Electronic component failure

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
94	Supports OTDT RX trip, OPDT RX trip, Rod Block, Lo Tave Feedwater isolation, Tave for Pressurizer level control and Steam Dumps.	7300 Processor support module (Integrator/computation module)	2 Lead/Lag amplifier cards (NLL), 1 Summing amplifier card (NSA)	NI (The failure could not be duplicated in the laboratory)	Erratic Output (Loop Delta T)	Control room received “DT Rod Withdrawal BLK Alert” “Bank Insert Low,” “OP DT RX Pretrip.”	Unit 1 control room received several alarms including “Rod Withdrawal BLK Alert”, “Bank Insert Low Alert” and “Rx Pretrip” when DeltaT and Tave in loop 3 spiked to 110% power on computer point. Loop 3 DeltaT and Tave were declared inoperable. 2 NLL cards were replaced with ASIC counterparts.	Electronic component failure
95	Supports OTDT reactor trip, OPDT reactor trip, rod blocks, Lo-Tave Feedwater isolation, Tave for Pressurizer level control and Steam Dumps.	7300 Processor support module	Summing amplifier card (NSA)	Shorted operational amplifier. OPDT (Loop 4) setpoint failed high.	Erratic Output	Loop 4 DeltaT and Tave were declared inoperable.	Loop D Over Power Delta Temperature (OPDT) setpoint failed high due to a failed NSA card. The output of the card was found saturated high; and the failure was understood to be due to a failed operational amplifier (OP-AMP), which had shorted internally.	Electronic component failure
96	NI	7300 processor support module. Signal Comparator Card (NAL)	NI	Intermittent Loss of Power	Failed to operate on demand	Control Room received “Safety Injection Bistable” and associated annunciator for Pressurizer Pressure “LO SI ALERT.”	While Unit 1 at 100% power, Control Room received channel “Safety Injection Bistable” and associated annunciator for Pressurizer Pressure “LO SI ALERT.”	Equipment Aging

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
97	RPS Overpower/ Over-temperature Delta- Temperature (OPDT/OTDT) Channels.	7300 Processor support module. Summing Amplifier Card (NSA) Used for temperature average conditioning	Operational amplifier on card	Failed output (HI or LO)	Erratic Output	Inoperable channel	While Unit 1 at 100% power, the OPDT Loop 3 setpoint increased automatically 119% with no alarms generated from this failure. Analysis of the component revealed that the output of Operational Amplifier (OP-AMP) was at zero with known input. The NSA card was replaced with an ASIC counterpart.	Cold/bad solder joint.
98	Steam generator level control	7300 Processor support module	Multiplier Divider Card (NMD)	Degraded pulse-to- analog converter signal	Erratic Output/ Loss of Indication	Control Room received "Steam Generator Flow Mismatch" annunciation.	While Unit 1 at 100% power, Control Room received "Steam Generator STM/FW Flow Mismatch" annunciation, which indicated that Steam Flow indication had failed low. Failure analysis showed that the failure was due to a degraded pulse to analog converter which provides a feedback to the input summing junction to stabilize the card's output. Replaced NMD card with new ASIC card.	NI
99	Over-temperature Delta temperature (OTDT) and Over-Pressure Delta- Temperature (OPDT) reactor trip channels.	7300 processor support module Summing Amplifier Card (NSA)	Transistor on the NSA card	short/ground	Erratic Output	OTDT setpoint dropped to approximately 20%.	Unit 2 Loop 3 OTDT setpoint dropped to approximately 20% causing OTDT and OPDT reactor trip bistables to illuminate. It was found that the failed component was a transistor on the NSA card.	NI

No.	Failure			Failure Mode	Effect		Event Description	Failure Cause
	System	Module	Component		Module Level	System Level		
100	RPS Overpower/ Over-temperature Delta- Temperature (OPDT/OTDT) Channels	7300 Processor support module	Resistance Temperature Detector (RTD) Amplifier Card (NRA)	NRA card failure (Actual failure mode not indicated)	Erratic Output	Control Room received multiple alarms that indicated a failure of a Delta-T and Tave for approximately 15 seconds, and then alarms cleared.	<p>Unit 2 Loop 4 Tcold dropped 20°F causing reactor pre-trip signals and alarms. Trends showed that Tcold signal dropped approximately 20°F for 15 seconds and then returned back to normal. The fault tree indicated that the most likely fault was the NRA card.</p> <p><u>OE Notes:</u> A review of industry events for the NRA card in the last 8 years revealed that the most common cause of failures appear to be random with no specific failure mechanism identified. Common experienced failure modes are drift high, drift low, fail high, fail low and erratic output from these failures.</p> <p>They were all considered random and had no specific failure mechanism</p>	NI

^aAST's are a form of software interrupt that is used to track I/O operations, and redirect flow based on the completion of this I/O.

INTERNAL DISTRIBUTION

1. Sacit M. Cetiner
2. Kofi Korsah
3. Gary T. Mays
4. Timothy McIntyre
5. Michael D. Muhlheim
6. Willis Poore III
7. Richard Wood
8. ORNL Office of Technical Information
and Classification

EXTERNAL DISTRIBUTION

9. Sushil K Birla, NRC
10. Thomas E. Burton, NRC
11. Khoi H. Nguyen, NRC
12. Daniel J Santos, NRC
13. Russell B. Sydnor, NRC