ELECTRIC POWER RESEARCH INSTITUTE

2013 TECHNICAL REPORT

Preventive Maintenance Practices for Digital Instrumentation and Control Systems

Preventive Maintenance Practices for Digital Instrumentation and Control Systems

3002000502

Final Report, August 2013

EPRI Project Managers
J. Naser
A. Hussey

All or a portion of the requirements of the EPRI Nuclear Quality Assurance Program apply to this product.

YES [✓ NO]

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Northrop Grumman Commercial Energy Corporation

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS **NOT** SUBJECT TO THE REQUIREMENTS OF 10 CFR PART 21.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Northrop Grumman Commercial Energy Corporation
7301 Sykesville Road
Sykesville, Maryland 21784

Principal Investigators
J. Maurio
C. McCarthy

This report describes research sponsored by EPRI.

The project team would like to thank the following people for their invaluable contributions to this report:

Hilina Abebe	Exelon Corporation
Robert Austin	EPRI
Michael Azarian	University of Maryland
Arnold Brewer	Exelon Corporation
Chaochao Chen	University of Maryland
Alan Dowell	Dominion Resources Services, Inc
Kenneth Dunham	Omaha Public Power District
Wesley Epperly	Northrop Grumman Maritime Systems
Scott Gladney	Tennessee Valley Authority
Jim Heishman	EPRI
Joshua Hemming	United States Navy
Raymond Herb	Southern Company
Mike Hudson	Ameren Corporation
Ron Jarrett	Tennessee Valley Authority
Wayne Johnson	EPRI
Tom King	FirstEnergy Nuclear
Jaeki Lee	KHNP
John Lijoi	Entergy Corporation

This publication is a corporate document that should be cited in the literature in the following manner:

Preventive Maintenance Practices for Digital Instrumentation and Control Systems. EPRI, Palo Alto, CA: 2013. 3002000502.

Tony Maselli	Invensys
Paul McCutchan	South Carolina Electric and Gas Company
Vince Mellens	Exelon Corporation
Joe Montgomery	Ameren Corporation
Scott Patterson	Pacific Gas & Electric Company
Michael Pecht	University of Maryland
Karl Sturzebecher	United States Nuclear Regulatory Commission
Justin Thibault	EPRI
Ray Torok	EPRI
David Valleroy	DTE Energy
Rick Way	EPRI
Peter Welch	Dominion Resources Services, Inc
Jonathon Williams	Exelon Corporation
Tony Williamson	American Electric Power

PRODUCT DESCRIPTION

The lack of industry-accepted preventive maintenance (PM) guidance for digital instrumentation and control (I&C) systems may be leading to failures and inadequate maintenance activities, which may be insufficient or overly conservative. Nuclear plants are installing digital components and I&C systems, especially for non-safety-related applications. In some cases, the PM practices being used are the same as or minor modifications of the practices used for analog equipment and systems. However, the new digital systems are very different from the analog or early digital systems, including new technology and components. The Electric Power Research Institute (EPRI) has collected data on digital I&C systems related to the performance of PM from nuclear power plants and other industries. These data are analyzed and recommendations are given based on the data and other experience.

Background

Nuclear power plants have implemented and are implementing digital I&C systems to address obsolescence issues, improve reliability and availability, and reduce operations and maintenance costs. Often, the system owners attempt to adapt their existing PM procedures for the original equipment to the new systems. Given that digital equipment behaves much differently from its analog predecessors, this PM strategy does not always provide optimal results. Some plants have been using digital equipment for over two decades and have developed thorough PM procedures and processes. Given the relatively small installed base of digital I&C equipment in the nuclear power industry, system owners can benefit from the experiences of other plants within and outside the nuclear power industry. Because of the increased implementation of digital I&C within the nuclear power industry, EPRI determined that a report that investigates the need for PM, the current practices, and recommended activities was needed.

Objectives

The primary objectives of this project were to:

- Collect and assess current PM tasks
- Identify weaknesses
- Recommend PM strategies for digital I&C systems

Approach

The project team used existing information available through various government and private agencies/corporations and from interviews with plant personnel responsible for the PM of digital I&C systems. Personnel from both within and outside the nuclear power industry were consulted about PM practices and experience. Additionally, interviews with personnel employed by manufacturers of digital I&C equipment were conducted.

Data from the Nuclear Regulatory Commission (NRC), the Institute of Nuclear Power Operations (INPO), and EPRI were used to establish the types of failures that occur with digital I&C equipment and any trends with those failures. Information from the various interviews was used to collect the current state of PM activities as well as best practices to be shared with the nuclear I&C community.

The project team evaluated the compiled information, taking into account the team's experience with military and commercial digital I&C systems. The approach taken considered the entire life cycle of the equipment, including recommending proper PM to ensure the longevity of the equipment. Such PM recommendations were developed based on capabilities of the equipment, component failure analysis, and operating experience in both land- and sea-based platforms.

Results

Failure data for digital I&C systems from the NRC, INPO, and EPRI were categorized by type of failure. The compiled data from 2008–2012 showed that human performance (averaging about six events per year) and hardware failure (averaging about four and one-half events per year) were the two most prevalent causes for digital I&C failures—that these were the top two is consistent with reported data for earlier years.

Many of the nuclear power industry respondents, as well as those outside the nuclear power industry, reported similar PM activities for their digital I&C systems. This, coupled with the relatively low number of hardware failures reported annually, suggested that for the most part, the proper PM is being performed on these systems. However, looking at the best practices of other plants and other industries as well, the additional PM recommendations could be used by plants to modify their PM activities to be more effective and potentially reduce failures.

Applications, Value, and Use

The report is intended for plant owners and maintenance and plant engineers. It identifies PM activities being used at plants and provides additional PM recommendations. Plants can compare this information with their own maintenance programs to determine if they want to modify their programs.

Keywords

Diagnostics
Digital system maintenance
Digital systems
Human-machine interface
Instrumentation and control systems
Preventive maintenance

EXECUTIVE SUMMARY

As of May 2012, the average age of a U.S. commercial nuclear reactor was 32 years [1]. Many of the original instrumentation and control (I&C) systems have outlived their useful life and are being replaced with modern versions. Most often, the replacement system is a digital system (consisting of processors, programmable logic controllers [PLCs], or field-programmable gate arrays [FPGAs]) running software or firmware), even if the original system was analog. A key reason for this is that digital systems can provide reduced operations and maintenance costs as well as improved plant availability during maintenance [2]. In addition, digital technology is the technology that is more likely to be available and more likely to be supported.

For many utilities and nuclear plants, modern digital I&C systems are still relatively new acquisitions. Often, these system owners attempt to adapt their existing maintenance procedures for the original equipment to the new systems. Digital equipment behaves much differently from its analog predecessors, so this maintenance strategy does not always provide optimal results. Some utilities and plants have been using digital equipment for over two decades and have developed thorough maintenance procedures and processes. Given the relatively small installed base of digital I&C equipment in the nuclear power industry, system owners can benefit from the experiences of other plants within and outside the nuclear power industry.

Because of the increased implementation of digital I&C within the nuclear power industry, the Electric Power Research Institute (EPRI) determined that a report that investigates the need for preventive maintenance (PM), the current practices and recommended activities should be developed. The work documented in EPRI report 1022713 [3] was begun to research the proper maintenance required for digital control systems in the nuclear power industry and is the genesis for the work presented here.

The primary objectives of this study were 1) to collect and assess current PM tasks, 2) to identify weaknesses, and 3) to recommend PM strategies for digital I&C systems.

Results

Failure data for digital I&C systems from the Nuclear Regulatory Commission (NRC), EPRI, and the Institute of Nuclear Power Operations (INPO) were categorized by type of failure. The compiled data showed that human performance and hardware failure were the two most prevalent causes for digital I&C failures. An average of four to six events per year for each of these categories has been observed over the past five years.

Many of the nuclear power industry respondents, as well as those outside the nuclear power industry, reported similar maintenance activities for their digital I&C systems. This, coupled with the relatively low number of hardware failures reported annually, suggested that for the most part, the proper maintenance is being performed on these systems.

One recommendation for improvement was to increase training for system maintainers in the use of vendor-supplied monitoring and diagnostics features. Through interviews with both the system owners and the equipment manufacturers, it appeared that the built-in monitoring and testing provided by manufacturers was not always used to the fullest extent. This can be due to not only unfamiliarity with the equipment and its capabilities but also limitations imposed by the application of the equipment in a nuclear power plant. Providing this training has the potential to reduce the number of system failures due to hardware failure observed within the industry.

A further recommendation was to use maintenance activities as opportunities to bolster other plant processes that are used to prevent system failures. For example, one respondent reported that when they replaced power supplies as part of their routine maintenance program, they also verified that the configuration of the new device matched that of the one being replaced, as well as the configuration provided in plant documentation. As a result, this activity provided an additional check to prevent system failure as a result of a configuration management or human performance issue. As this example illustrates, a side benefit of using maintenance activities as an opportunity to check or verify against multiple types of digital system failures is that it has the potential to catch many other types of digital system issues before they manifest themselves as failures.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

As of May of 2012 the average age of a US commercial nuclear reactor was 32 years [1]. Many of the original instrumentation and control systems have outlived their useful life and are being replaced with modern versions. Most often, the replacement system is a digital system (consisting of processors or PLCs running software or firmware) even if the original system was analog. A key reason for this is that digital systems can provide reduced operations and maintenance costs as well as improved plant availability during maintenance [2]. In addition, digital technology is the technology that is more likely to be available and more likely to be supported.

For many utilities and nuclear plants, modern digital instrumentation and control (I & C) systems are still relatively new acquisitions. Often, these system owners attempt to modify their existing maintenance procedures for the original equipment to the new systems. Digital equipment behaves much differently from its analog predecessors so this maintenance strategy does not always provide optimal results. Some utilities and plants have been utilizing digital equipment for over two decades and have developed thorough maintenance procedures and processes. Given the relatively small installed base of digital I&C equipment in the nuclear power industry, system owners can benefit from experiences of other plants within and outside of the nuclear power industry.

Because of the increased implementation of digital I&C within the nuclear power industry, EPRI determined that a report that investigates the need for preventive maintenance, the current practices and recommended activities needed to be developed. The work documented in Reference [3] was begun to research the proper maintenance required for digital control systems in the nuclear power industry and is the genesis for the work presented here.

The primary objectives of this study are 1) to collect and assess current preventive maintenance tasks, 2) to identify weaknesses, and 3) to recommend preventive maintenance strategies for digital information and control systems.

This study was executed using existing information available through various government and private agencies/corporations and interviews with utility and plant personnel responsible for the maintenance of digital I&C systems. Personnel from both within and outside of the nuclear power industry were consulted about maintenance practices and experiences. Additionally, interviews with personnel employed by manufacturers of digital I&C equipment were conducted.

The data from the NRC, EPRI and INPO was used to establish the types of failures that occur with digital I&C equipment and any trends with those failures. Information from the various interviews was used to collect the current state of maintenance activities as well as best practices to be shared with the nuclear I&C community.

The compiled information was evaluated from the perspective of a major designer and manufacturer of military and commercial digital instrumentation and control systems. This perspective includes an approach that considers the entire lifecycle of the equipment, including recommending proper maintenance to ensure the longevity of the equipment. Such maintenance recommendations are developed based on capabilities of the equipment, component failure analysis and operating experience in both land- and sea-based platforms.

2
THE NEED FOR PREVENTIVE MAINTENANCE OF DIGITAL I&C SYSTEMS

Digital systems have the ability to overcome many of the limitations associated with analog electronics, but they still require routine maintenance. According to a survey of the nuclear power industry, most existing preventive maintenance activities for digital instrumentation and control systems are based on a combination of the maintenance activities of the analog systems that the digital electronics have replaced, the maintenance requirements for analog components that interface to the digital system and to a lesser extent the preventive maintenance requirements of the installed digital system [3].

Digital System Failure Modes

In order to better appreciate the need for the various maintenance activities required for digital I&C systems, it is instructive to look at the ways in which digital equipment can fail. Failure modes are the ways or manners in which the digital electronics failures are observed. They are the manifestation of the defect or failure within the electronics. This is in contrast to failure mechanisms which are the processes that caused the failure.

Digital electronics can be examined at the lowest levels, integrated circuit chips and components, through intermediate assemblies such as circuit cards and modules to entire systems. In many cases, the failure mode for the electronics is either a short or open circuit (other modes consist of items such as changes in leakage current, cracks, and delamination) [4].

Digital Integrated Circuits, Memory, Processors and FGPAs

In computer or processor-based systems, failure modes manifest themselves in various ways. Internal to integrated circuits, including memory, processors and FPGAs are wires within the package (bond wires) that may fail open and prevent the proper signal from interfacing with the devices pins. Alternatively, a wire may come loose and contact another wire or conductor on the chip itself, leading to incorrect behavior or damage. It is also possible that one or more of the chip’s internal transistors or circuit paths may fail. As a result of any of these actions, digital integrated circuits can have input and output data become altered between the pins and chip (e.g. stuck bits, data bit loss, high leakage current) [5].

Additionally the chip itself may fail to interface correctly with external devices and components. If the failure is in memory, a request by the processor for information may be returned incorrectly or the processor may read an incorrect instruction from memory and execute its program incorrectly possibly causing the processor to run in a loop or stall [5].

As digital integrated circuits continue to be scaled to smaller sizes, certain other faults are emerging such as transient faults due to radiation particle strikes and faults that lead to a degradation of performance of the circuit as opposed to an outright failure. Some of these degradation faults are digital speed degradation and FPGA delay increase as a result of time-dependent dielectric breakdown of gate dielectrics and negative bias temperature instability. Studies are showing that in some cases, scaling of the integrated circuits is decreasing reliability [6].

Data Communication

Data communication is critical to most digital instrumentation and control systems. Often, the control electronics and sensor interface circuitry is distributed among several locations and accurate and timely information exchange between the various components is critical for proper and safe operation. Communication errors identified in IEC 61784-3 are as follows:

- Data corruption
- Unintended repetition
- Incorrect sequence
- Data loss
- Unacceptable delay
- Insertion
- Masquerade
- Addressing [5]

Examples of communication faults identified in NRC DI&C-ISG-04 [7] include:

- Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
- Messages may be repeated at an incorrect point in time.
- Messages may be sent in the incorrect sequence.
- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
- Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
- Messages may be inserted into the communication medium from unexpected or unknown sources.
- Messages may be sent to the wrong destination, which could treat the message as a valid message.
- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
- Messages may contain data that is outside the expected range.

- Messages may appear valid, but data may be placed in incorrect locations within the message.
- Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
- Message headers or addresses may be corrupted [7].

Support Electronics

Other failures associated with digital instrumentation and controls systems are related to the support electronics for the processor and memory. These include power supplies and interface circuitry as well as some of the components on the processor or system circuit board itself.

Power semiconductors (diodes, MOSFETS, SCRs, IGBTs, etc.) are found in most power supplies, battery chargers, inverters and rectifiers and in some cases on individual printed circuit boards to create various voltages to distribute to the integrated circuits on the card. The typical failure modes for power semiconductors are open circuit, short circuit and high leakage current. The particular failure mode depends on the type of component and the electrical and environmental stresses applied to the device [8] [9].

Magnetic components (such as power transformers, instrumentation transformers and chokes or inductors) are utilized in digital control and instrumentation systems. In the absence of a manufacturing defect or high environmental or electrical stresses, these components typically do not fail [8]. If a failure of a transformer does occur, it will most likely develop an open circuit (although shorted turns do sometimes occur) [9]. Often in electronic cabinets designed for the military, the larger magnetic components are placed in the back or bottom of the cabinet, where they are relatively inaccessible. This is due to the high probability of these components never needing to be serviced during the life of the equipment.

Electrolytic, tantalum and film capacitors are commonly used within digital instrumentation and control hardware. Failure modes for capacitors include short circuit, open circuit, reduction in capacitance and increase in equivalent series resistance. Industry failure data indicates that capacitor failures are predominantly dc aluminum electrolytic capacitors [8][10].

Circuit board failure modes consist of complete loss of function, partial loss of function and reduced performance. Catastrophic failures of circuit boards that have undergone a “burn-in” period are rare [8].

The common failure mode for a fuse is an open circuit when not expected or intended or a slow to occur open circuit [11].

Software

In general, software faults have the same effects as hardware faults in processors or memory. Although improving rapidly, the ability to evaluate software faults and any resulting effects is still in its infancy compared to the ability to evaluate hardware faults. This report focuses on maintenance activities for digital systems and so it should be noted that maintenance is not typically performed to detect software faults. These are more appropriately addressed during design and development particularly through vendor-performed software Verification and

Validation (V&V) testing, Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT) and commissioning.

Digital System Failure Mechanisms

Digital system failures may arise from one of three categories: hardware faults, software faults and systematic faults.

Hardware Faults

Most of the failure mechanisms identified for printed circuit boards are generally applicable to digital I&C systems as these systems consist predominantly of packaged printed circuit boards. Reference [12] provides a list of printed circuit board and electronic component failure modes and mechanisms in Table 4-2. An additional failure mechanism that has been observed for printed circuit boards, although infrequently, is metal whisker growth leading to partial or complete loss of functionality of the circuit board. Appendix A provides a more thorough discussion on the causes, effects and prevention strategies for metal whiskers within electronic circuits.

There are several stressors that can lead to or accelerate hardware faults. These are thermal stresses, electrical stresses, mechanical stresses, electromagnetic interference, humidity, atmospheric pressure and salinity [6][8]. With the exception of periodic replacement of components, typical digital system maintenance activities are directed towards monitoring or reducing the environmental stressors that can accelerate or cause hardware faults. The following section therefore, describes the various stressors that can promote or cause hardware faults along with the failure mechanisms that they may contribute to.

Thermal Stresses

Thermal stresses, including operation at high temperature as well as thermal fluctuation are a common cause for electronic component failure. Electronics are designed by the manufacturer to operate in specific ambient temperature ranges. As long as the devices are operated within their rated temperature ranges, failures are rare. Operation outside these ranges, particularly operation above the rated ranges increases failure rates. According to studies performed by the Los Alamos National Laboratory, failure rates double for every rise of 10° C (18° F) [13].

Many power electronic devices produce a large amount of heat as a result of their operation. They typically are provided with a method or device such as a forced air, fan, heatsink, or heatpipe to reject this heat to the environment. Higher ambient temperatures will reduce the ability of the heat removal mechanism to keep the device cool.

High ambient storage temperatures will accelerate the aging of electrolytic capacitors, with the rate of aging primarily determined by the storage temperature and the selection of materials and quality of construction [10].

High thermal stresses (including temperature cycling) can lead to connector wear or breakage for printed circuit boards [12]. Temperature cycling can also cause stress-related failures in processors particularly at the interface between the device package and the connection to the printed circuit board [14].

High temperature operation (higher than rated or recommended values) negatively impacts nearly all types of electronic and electrical components. Some examples of the detrimental effects of high temperature operation are (in no specific order):

- Total or partial failure of printed circuit boards due to changes in the physical properties of its constituent electronic parts. The dominant stress causing electrical components and circuit boards to fail is heat [8].
- Shorted or open circuit for power electronic devices due to junction overheating. Loss of capacitance or open circuit due to degradation and/or loss of electrolyte in electrolytic capacitors.
- Open circuit for fuses. Coil burnout in relays [15].
- Increase in the rate of electromigration and time-dependent dielectric breakdown in microprocessors [14].
- Turn-to-turn shorts or open circuits for magnetic components due to degradation of insulation.

Electrical Stresses

Electrical stresses, including high harmonics on power lines and power surges are another source of damage to digital equipment [6]. This is particularly true for power supplies, inverters and battery chargers as they interface directly to the power lines.

High harmonics can lead to excessive heating of cables and transformers. They can cause increased power dissipation in certain electronic circuits. The increased heating can lead to shortened lifespans of electrical components.

Surge voltages through power semiconductors increase the current through the device and thus the power dissipation creating more heat. Because the change in the current through the device is rapid, there may not be sufficient time for the heat to be carried away by the thermal management system for the device due to the long thermal time constants. This can lead to overheating of the device's junction. If the surges are applied repeatedly, the device may fail due to the resultant thermal cycling of the device and its packaging. Additionally, these surge voltages may be high enough to exceed the device's dielectric strength leading to breakdown [8].

Electrical stresses can lead to failure of magnetic components. Exposure to surge voltages and currents can cause overheating (if prolonged) and can also destroy the coil insulation through dielectric breakdown [8].

Overvoltages can cause electrode degradation and corona effects in capacitors leading to either a short circuit or increase in equivalent series resistance [8]. Prolonged overvoltage can lead to coil burnout in electromechanical relays and increased leakage current and output switching element failure in solid state relays [15].

Mechanical Stresses

Electronic equipment may be subjected to many different forms of vibration over various frequencies and at different acceleration levels. It may experience the vibration due to its proximity to nearby rotating or moving equipment. It should not be forgotten that the equipment may be subjected to vibration during its transport during and post assembly [6]. For terrestrial applications, such as nuclear power plants, vibration and shock experienced by the equipment may be due to seismic events.

Due to the mechanical properties of solder, solder joints on printed circuit boards are prone to failure in high vibration environments. Circuit card connectors (card edge and plugs and jacks) can wear-out from repeated vibration and high number of insertion and removal cycles [8].

In general, vibration of electronic equipment has the potential to loosen electrical connections and short circuits if exposed conductors or conductive surfaces are free to move. Vibration can loosen electrical terminations and magnetic core and cause dielectric breakdown of embrittled insulation. According to [8], however, not many instances of this failure have been reported in the industry. Vibration can lead to intermittent contacts, breaking of contact to case connection and pickup and dropout voltage shifts from misalignment in relays [15].

Electromagnetic Interference (EMI)

Electromagnetic interference is a result of unwanted electromagnetic emissions from a device or circuit that interferes with the normal operation of another device or circuit. When current flows through a conductor it generates an electromagnetic field. This field can radiate out from the conductor and be intercepted by another conductor or circuit. Therefore, any electrical circuit or component is a potential source of EMI. Devices within the receiving or “victim” circuit may be negatively impacted by the EMI and lead to increased noise levels or voltages that cause equipment malfunction [6].

Interference clustered around a single frequency (narrowband interference) usually results from an intentional transmitter such as a radio, cell phone or a Wi-Fi router. It is often easier to discover the source of this type of interference as typical transmission frequencies of intentional transmitters are well known.

Interference spread-out over a wide range of frequencies (broadband interference) is typically from unintended transmitters and is a secondary result of the operation of circuit from which it emanates. Typical sources include nearby power lines, electric motors, relays, especially when switching inductive loads, welders, computers and digital circuits with high clock frequencies.

In addition to interference resulting from radiated electromagnetic waves, it is possible for circuits to experience interference from physical contact with a circuit. This is referred to as conducted electromagnetic interference. For example, if ac power to a circuit contains excess electrical noise then this can negatively impact the operation of the circuit [6]. Reference [16] provides a discussion of the type and level of EMI typically present in a nuclear power plant.

Humidity

Electronics can be adversely affected by both high and low humidity levels. High levels of humidity can lead to condensation on electrically conductive surfaces which may cause unintended short circuits or can lead to increases in leakage currents for electronic components. High humidity can also accelerate chemical reactions that contribute to corrosion of the equipment.

Very low levels of humidity increase the chance for the build-up of charges within the equipment which can lead to electrostatic discharges. These discharges can cause dielectric breakdown within electronic component [6].

In addition to ambient humidity conditions, lowering the temperature within a room, cabinet or chassis can increase the relative humidity within. Excessive cooling of the environment containing the electronics can lead to water condensing on the equipment.

Atmospheric Pressure

The effects of atmospheric pressure on electronics are typically only of consequence at high altitudes where the air density is very low. Low atmospheric pressure can reduce the ability of thermal management system to effectively transfer heat from the electronics resulting in higher than normal operating temperatures [6].

Salinity

Salinity affects electronics devices used in coastal regions, ships and marine applications and nuclear plants near large bodies of salt water. The primary mechanism regarding salinity that impact electronics is the resulting corrosion of conductors due to the salt and the degradation of insulating material as salt collects on the surface that can increase the surface conductivity of the insulation [6].

Software Faults

There are three sources of failure of software: application software, system software and development software. Within each of these, errors can be attributed to three main causes. The first is when a problem is caused when critical information is not included or utilized in the software. These are called errors of omission. These types of errors are commonly associated with missing information in requirements or specification documents, actual computer code and documentation [17].

The second type is referred to as an error of commission. This is an error that results of an incorrect action that has been taken. This error is often encountered during the design and coding phases of the software [17].

The third type of software fault is an error of clarity or ambiguity. As the name suggests, these are errors resulting from an incorrect interpretation of information. They can result from vague requirements being provided to the software development team [17].

These errors can be introduced at any stage of the software development lifecycle. Rigorous testing both pre- and post-installation is designed to discover all of these errors. However, in practice, it is nearly impossible to find all of these errors due to the often complex nature of the digital system and its associated software. Commonly, a system will function normally for a period of time until a certain condition occurs (trigger) that “activates” the software error [5]. It is important to note that software itself does not experience any aging mechanisms. A failure of a digital system may occur as a result of a software fault that has been challenged by an activating condition. Developers of digital I&C equipment employ extensive testing to both locate and eliminate software faults before delivery to the customer. Additionally, for critical applications, systems are architected to minimize the potential for, and impact of, the activation of a software fault [18].

Research shows that a majority of software errors for safety-critical systems are the result of errors in the requirements for the software. This results from specifications that are incomplete, incorrect or ambiguous, that is a combination of the first and third type of errors described above [18]. Maintenance activities are not intended to uncover software faults (these are reserved for vendor and customer acceptance tests). Certain maintenance activities (particularly application level and system level tests) do provide additional opportunities to uncover undetected software faults possibly reducing the probability of these faults leading to failures during operation. However, the success of this detection is largely subject to happenstance.

Systematic Faults

Systematic faults are faults that are attributed to an error in the design, manufacturing and use of the equipment. A systematic fault is a “designed-in” flaw that will yield the same failure or misbehavior every time the same triggering conditions are present. Systematic faults can also be due to factors that were not considered or addressed in the design and development process such as environmental conditions that exceed the recommended operating conditions.

Software faults are sometimes considered to be systematic faults as software does not “fail” or suffer from wear-out mechanisms and are therefore due to errors in the design and development process [5]. In principle it would be possible to avoid all systematic faults by applying rigorous quality processes during development and testing, maintaining proper operating conditions and the use of redundant and diverse system architecture.

Nuclear Power Industry Experience

Previous EPRI research has provided a comprehensive set of data regarding the failures and issues experienced with digital instrumentation and control systems within the nuclear power industry. EPRI report 1016731, Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems [19], provides a list of digital system failures compiled from several sources including Licensee Event Reports (LERs), Event Notifications (ENs) and INPO Operating Experience (OE) reports spanning 1987 through 2008. The report identified a total of 322 digital system events. Hardware failures were identified as the main cause for both 1E (safety-related) and non-1E (non-safety related) equipment as evident in Figure 2-1 and Figure 2-2 which are reproduced here from the EPRI report.

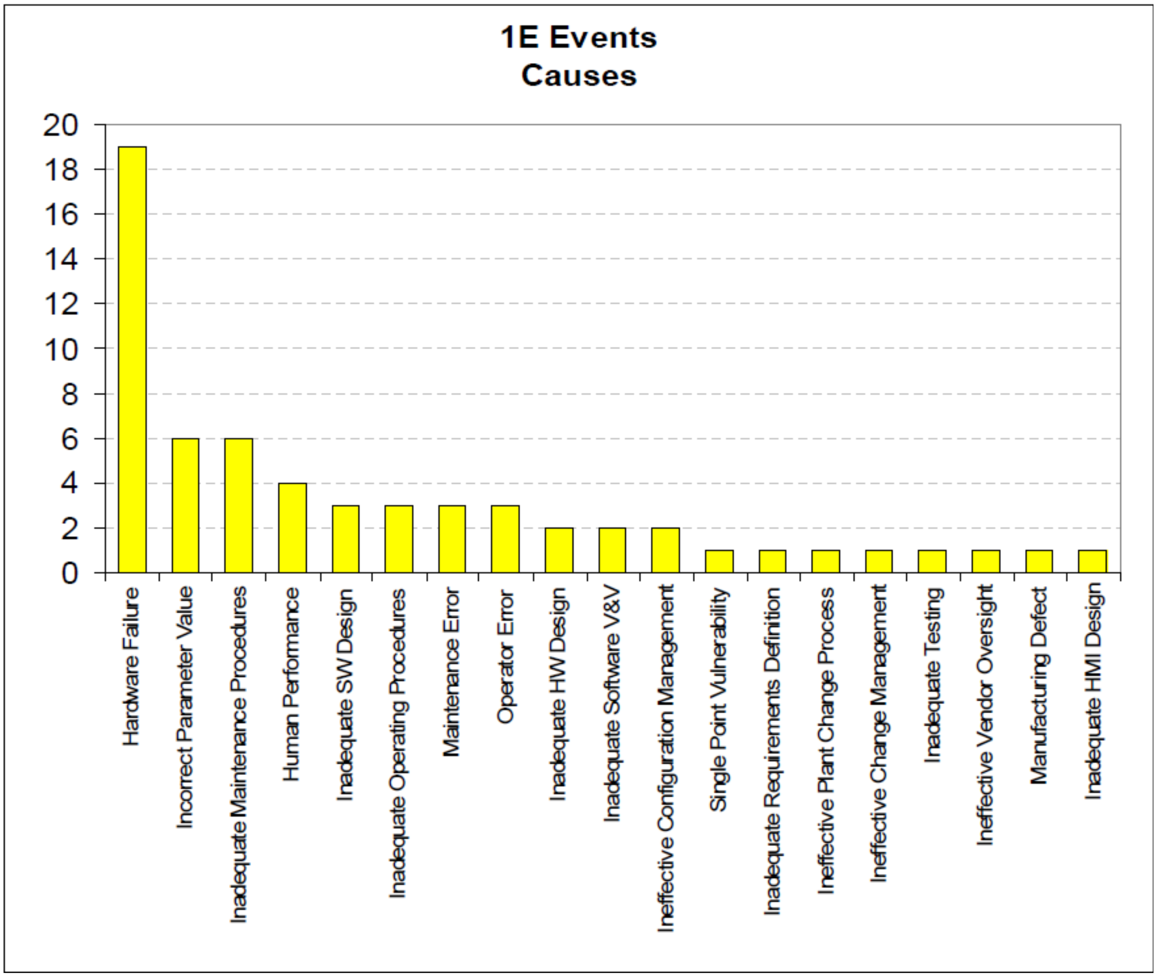

Figure 2-1
Causes of 1E Digital Failures from EPRI Report 1016731

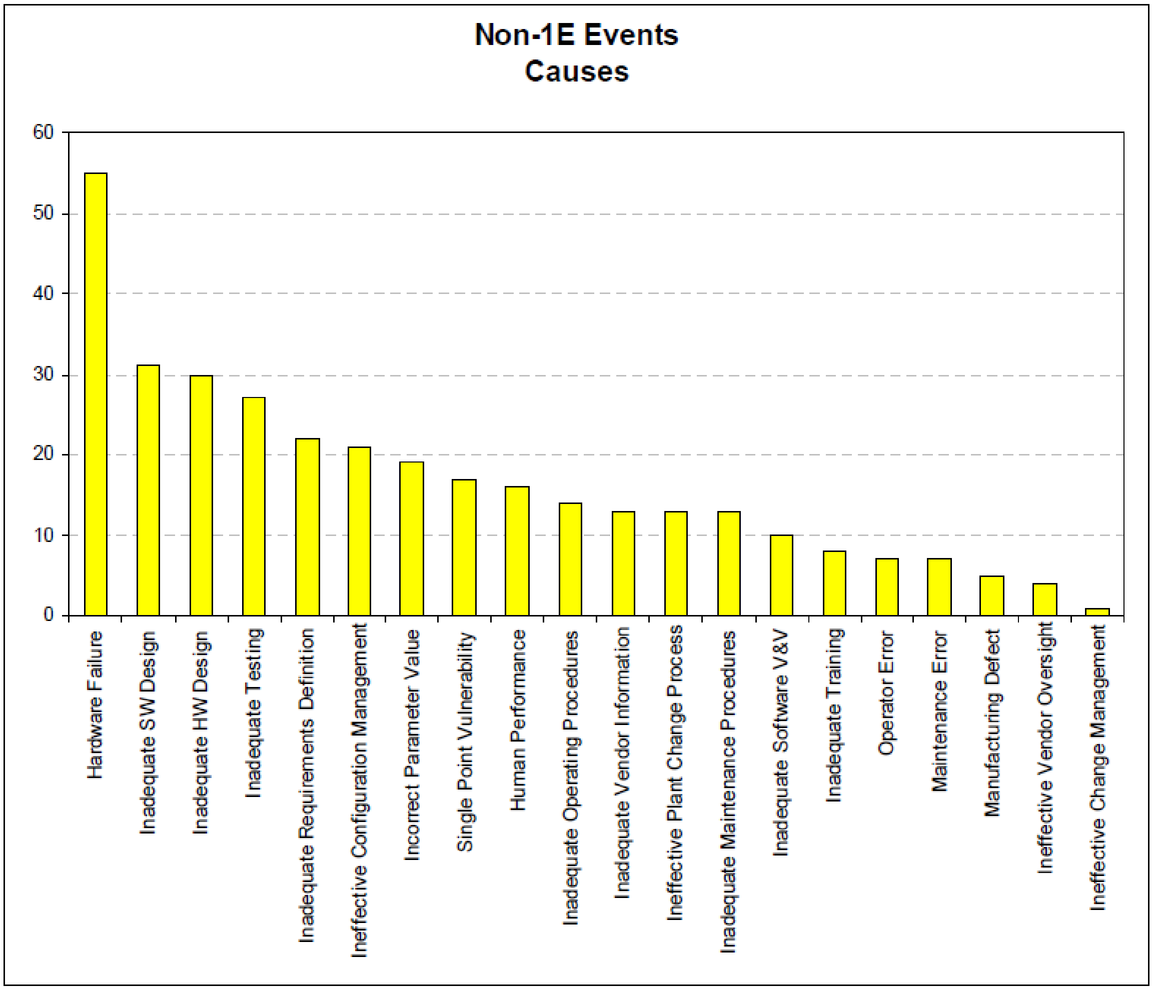

Figure 2-2
Causes of Non-1E Digital Failures from EPRI Report 1016731

Combining the date for both the 1E and non-1E systems, 21 categories of failures were identified as presented below.

1. Hardware Failure
2. Inadequate SW Design
3. Inadequate HW Design
4. Inadequate Testing
5. Incorrect Parameter Value
6. Inadequate Requirements Definition
7. Ineffective Configuration Management
8. Human Performance
9. Inadequate Maintenance Procedures
10. Single Point Vulnerability

11. Inadequate Operating Procedures
12. Ineffective Plant Change Process
13. Inadequate Vendor Information
14. Inadequate Software V&V
15. Operator Error
16. Maintenance Error
17. Inadequate Training
18. Manufacturing Defect
19. Ineffective Vendor Oversight
20. Ineffective Change Management
21. Inadequate HMI Design

An objective for the present study is to determine if there have been any significant trends in digital failures since EPRI report 1016731 was published. Any such trends might provide some insight into whether present preventive maintenance activities are being effective at reducing digital failures. To maintain consistency with the data presented in Figure 2-1 and Figure 2-2, it was decided to use the same categories for digital failure as used previously when analyzing the new data.

Upon closer examination of these categories, it was determined that Maintenance Error, Operator Error and Incorrect Parameter Value could all be considered as part of Human Performance errors since they all relate to an error in human behavior or activity. Additionally, it was decided to combine the categories of Ineffective Change Management and Ineffective Plant Change Process into a single category of Ineffective Change Management / Process. The categories of Inadequate Vendor Information and Ineffective Vendor Oversight were similarly combined into a single category of Inadequate Vendor Information / Oversight.

A baseline for comparison with the new data was created by combining the data for the 1E and non-1E equipment into a single set and reclassifying the failure types using the condensed categories discussed above. This data is presented in Figure 2-3.

It is interesting to note, that with the data combined and categorized as above, human performance related-causes now emerge as the second highest cause of digital events. This conclusion was not readily apparent from the two separate graphs of data using the larger number of categories.

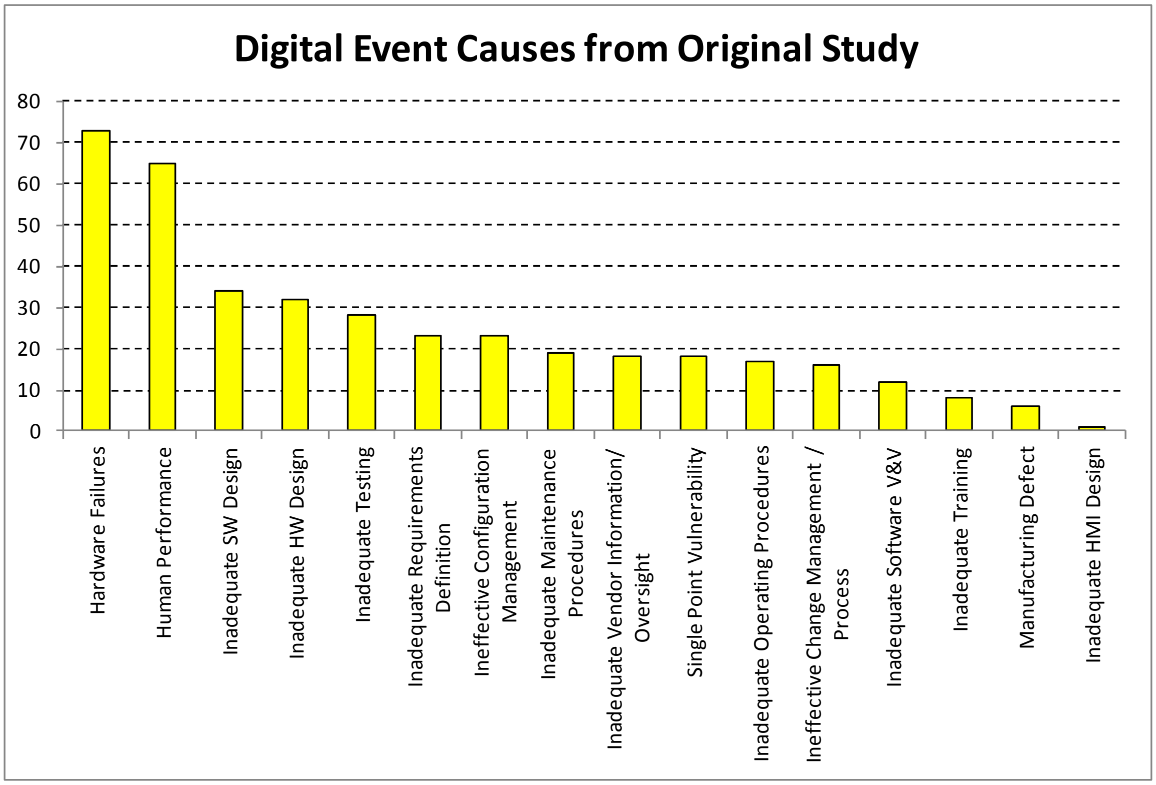

Figure 2-3
Causes of both 1E and Non-1E Digital Failures from EPRI Report 1016731

EPRI report 1016731 [19] was completed in 2008. Data from the NRC's Licensee Event Reports (LER) database and the Institute of Nuclear Power Operations (INPO) EPIX database covering the period of 2008 through 2012 was examined for digital system events. A keyword search was used to obtain a base set of data. The keywords search used was "digital OR computer OR software OR programming OR processor OR microprocessor OR firmware". This yielded 193 records from the LER database and 109 records from the EPIX database. Of these, 86 were events that specifically covered a failure of a digital system. For the purposes of this report, "digital" includes any system that contains a processor and/or is running software or firmware and that can have parameters entered or programmed by the user/maintainer. It should be pointed-out that the data from the previous EPRI report utilized a more inclusive definition of a "digital" system.

The resulting data was compiled using the same 16 categories of Figure 2-3 and is presented in Figure 2-4. From the data, it can be seen that human performance issues now are the predominant cause of digital failures. This is not necessarily an unexpected result as it is expected that modern digital equipment should be more reliable than those systems fielded twenty or thirty years ago thanks to improvements in manufacturing quality and built-in tests and diagnostic capabilities. Thus, one might anticipate that another cause of digital failure would overtake Hardware Failure as the primary failure. In fact, this reliability is one of the primary reasons that utilities choose to replace their aging systems with modern digital ones.

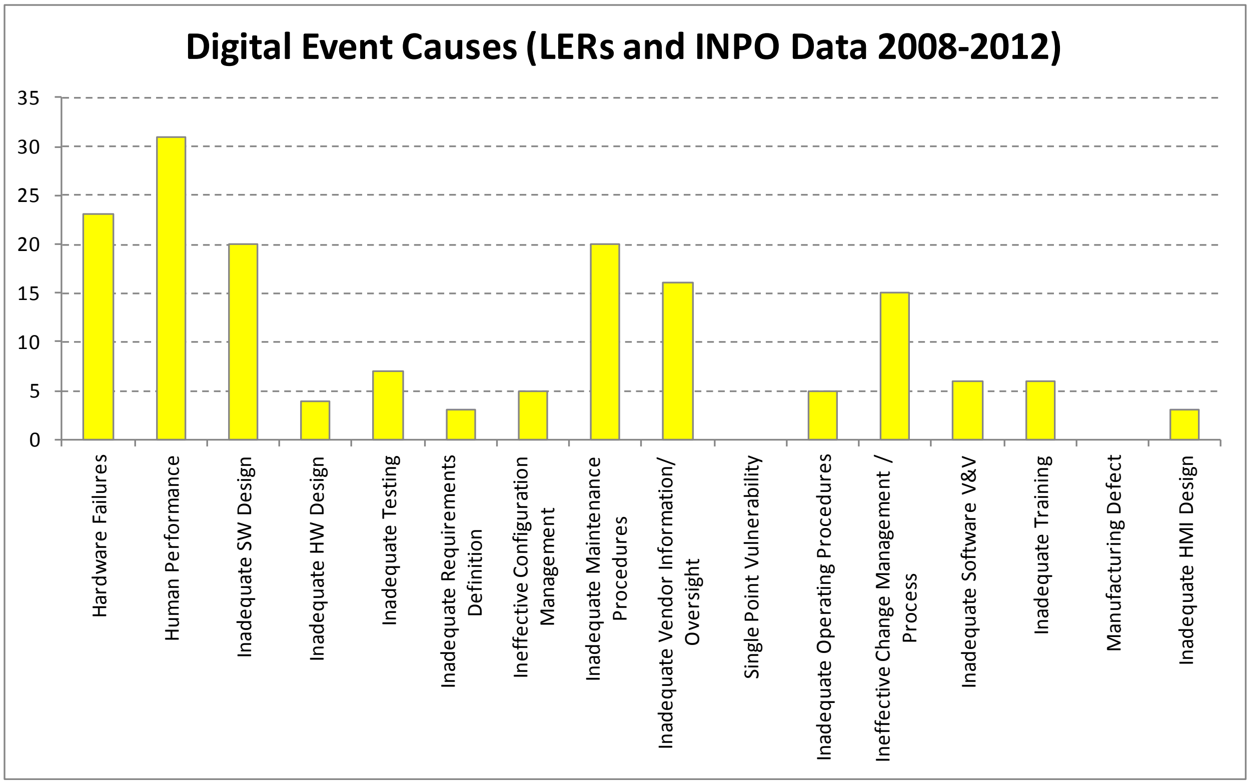

Figure 2-4
Causes of both 1E and Non-1E Digital Failures (2008 – 2012)

In order to determine if there is a trend in the quantity and types of failures that are occurring, the data from 2008-2012 presented above was organized by the year of the event (Figure 2-5). Human Performance and Hardware Failures are averaging around 5 or 6 per year, with no clear trend, either increasing or decreasing. The next highest categories, Inadequate Software Design and Inadequate Maintenance Procedures are averaging 4 per year. The time span under examination is somewhat brief, so it may be difficult to draw any significant conclusions. This data seems to indicate that the issues with digital instrumentation and control still remain largely the same (hardware failures and human performance), as each of these failure types is present in each of the years investigated.

Examining the Human Performance category further we find that in every year except 2008, Maintenance Error and Incorrect Parameter Value account for greater than 67% of the Human Performance category failures. That percentage, coupled with number of failures attributable to Inadequate Maintenance Procedures, suggest that it may be possible to modify maintenance practices to substantially reduce the total number of digital failures as these practices can have a direct impact on the first and third highest failure categories.

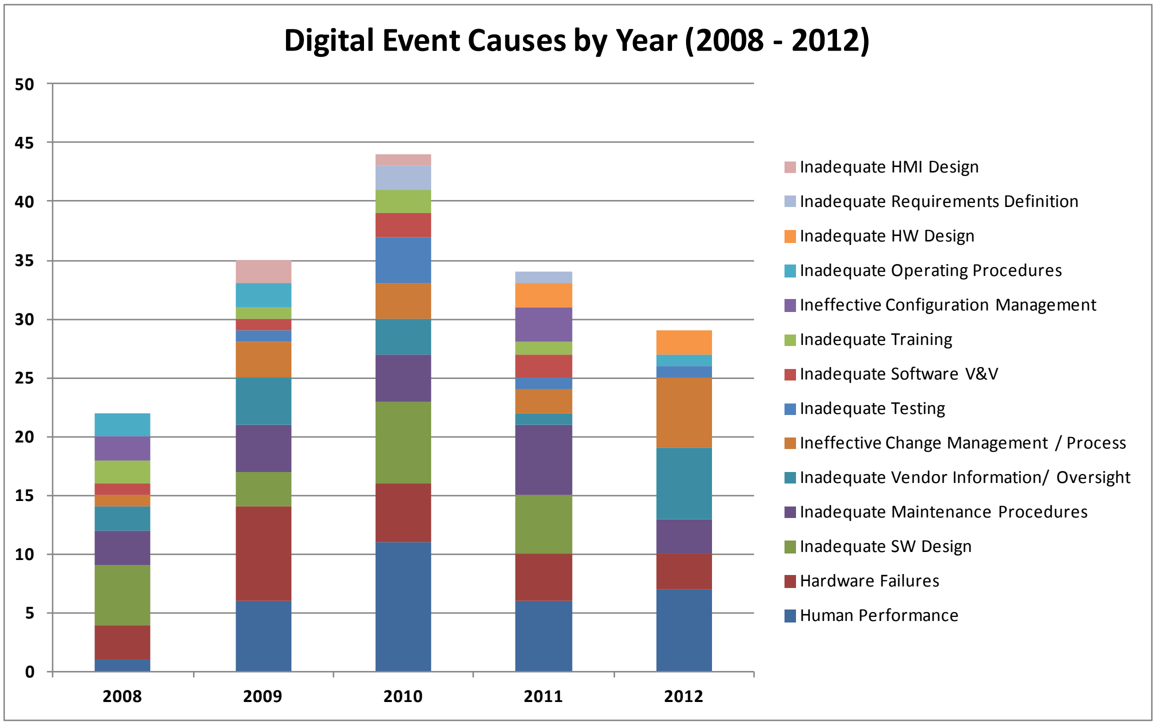

Figure 2-5
Causes of Digital Failures by Year (2008 – 2012)

Non-Nuclear Power Industry Experience

A search of the literature regarding digital failures of other safety-conscious industries such as aviation and rail transport was performed. The most comprehensive information found in the literature was in [5]. This report examined digital I&C failures in the petrochemical, aviation, public phone network in addition to domestic nuclear power plants. The most pertinent information was found in the aviation data.

The report examined the FAA’s Aviation Safety Information Analysis and Sharing (ASIAS) System. This database was searched for digital-instrumentation related incidents. Over 86,682 records were searched yielding 67 incidents that were digital/computer related. The listed causes of failures were, in order of greatest number to least number, General Computer-related Problem (18), Physical Failure (12), False Indication (11), Calibration Problems (10), Failed Execution (8), General Instrument Problem (4) and Accessory Failure (4). While it is difficult to map these causes directly to the categories presented above, it is can be seen that hardware failures (Physical Failure) and human performance (Calibration Problems) are two of the most prevalent causes. The authors note that there is a general trend toward fewer failures over the past few years although no reason is provided.

In addition to performing the literature search above, interviews with persons familiar with maintenance of digital systems in other industries were conducted for the current study.

Shipboard Machinery Controls

In general, modern machinery controls for shipboard applications consists of Programmable Logic Controllers (PLCs), HMI computers and network servers. Anecdotal evidence from the personnel familiar with the operation and maintenance of these systems, suggests that the biggest failures in these systems are not due to problems with the PLCs but rather the HMI computers and servers. Power supply and hard drive failures are common as well as circuit card terminal block failures and failures of relay output modules driving inductive loads without protection.

Shipboard RADAR, Communication and Data Systems

Shipboard RADAR, communication and data systems consists of combinations of rack-mounted processing gear, computers and cabinet mounted card cage assemblies. Personnel familiar with the operation and maintenance of these systems suggest, that, in general, if well maintained (kept cool, periodically inspected and cleaned) these systems are very reliable. Processor lock-ups and issues with UPSs are some of the common issues reported.

3

PREVENTIVE MAINTENANCE PRACTICES FOR DIGITAL I&C SYSTEMS

Types of Maintenance

The need for maintenance is based on the actual or impending failure of the equipment. Ideally maintenance is performed to keep equipment and systems running efficiently for at least the design life of the components. There are at least three types of maintenance models available to a system owner. These are: reactive maintenance, preventive maintenance and predictive maintenance [20][21].

Reactive Maintenance

This type of maintenance, also known as "run-to-failure" maintenance involves allowing equipment to operate until it no longer can perform its intended operation and must be repaired or replaced. A purely reactive maintenance program would not perform any maintenance actions on a piece of equipment until it ceases to perform its intended function or fails completely [20]. An entirely reactive maintenance program considers the possibility of failure of any piece of equipment within the system to be the same. No attempt at prioritizing equipment for maintenance activities is made because no actions are planned or taken to extend the life of the equipment. This approach does not take advantage of the ability to extend the life of the equipment through routine maintenance activities.

The disadvantages of this approach include:

- High percentage of unplanned maintenance activities.
- Potential high costs with unplanned or "emergency" repairs.
- Need for large inventory or replacement parts (higher capital cost).
- Possible inefficient use of maintenance staff.
- Possible collateral damage or shortening of life of connected equipment.

The advantages of this approach are:

- Reduced maintenance staffing.
- Possible reduced maintenance cost if the equipment is new or very reliable.

If the goal of a preventive maintenance program is to ensure that the equipment continues to perform its intended function and not simply to eliminate hardware failures within the system, then a reactive maintenance model can be an effective and economical strategy for digital I&C systems. This is particularly true if all (or at least the most critical) of the digital I&C systems are designed to be single failure tolerant, that is, a failure of any one component or module will not impede the overall functionality of the system. There may be a higher initial cost with architecting these systems with sufficient redundancy, but these should be offset by the reduced amount of surveillance and replacement maintenance activities.

Preventive Maintenance

The theory behind preventive maintenance is that by adjustment, inspection, cleaning, lubricating, informed parts replacement, calibrating and repair of components and equipment, failures can be reduced. Preventive Maintenance is also referred to as time-driven or interval-based maintenance. It is performed on a scheduled basis, without regard to equipment conditions [21].

Preventive maintenance defines that periodic inspection and maintenance be performed at pre-defined intervals. This inspection for suspect parts and/or the scheduled replacement of certain types of parts is intended to reduce equipment failures for equipment thought to or known to be susceptible to time-driven failures. While this approach leads to more inspections and routine maintenance, it is believed that the frequency of failures is sufficiently reduced to make this action economically attractive. This approach is particularly indicative when age wear-out mechanisms have been identified. Wear-out, per se, is a simple concept, but generally not very applicable to the failure of digital systems.

Setting a fixed time interval for replacement, can often result in unnecessary maintenance. Coupled with the possibility of mechanical damage or stress in replacing parts that are currently performing satisfactorily, timed maintenance should be used sparingly, and primarily on components that are well established to have aging mechanisms (such as electrolytic capacitors) [21]. Failure rate (number of failures per unit time) or its reciprocal, MTBF (time per failure), can be used to help establish maintenance intervals. MTBF is an often misunderstood concept. The misunderstanding is based on the reasonable (but incorrect) thought that failures will be uniformly distributed over time. In fact, while MTBF results may be based on excellent data, time between failures should be understood to be truly random. Furthermore stressors in the environment as discussed above can have a profound impact on failure rates. It would be unwise to expect that a component is likely to work satisfactorily until it reaches a time equal to its MTBF value; it is likely to be much more or much less.

The reduction in size for integrated circuits, processors and FPGAs is strongly influencing the reliability of modern digital systems. Issues with scaling have introduced several failure modes that are associated with degradation of the circuits as opposed to complete failure. This has lead to greater difficulty applying conventional reliability analyses based on these degradations [6] and thus complicates establishing MTBFs for this type of equipment.

It is also very difficult to determine the “correct” periodicity for preventive maintenance tasks. The best indicator would be data collected on the subject system itself. But since the environment is often variable, and the load and input voltages may also vary, even this “best” approach is seriously flawed. And by the time sufficient data to make a reasonable estimate is collected, the equipment is now in an aged condition, and the collected data may not even be representative. A better approach is to monitor the equipment and look for trends. Carefully collecting data periodically is a good practice. When a change in the rate of the trended data is indicated, the sampling period can be increased so that action can be taken before the performance of the equipment goes out of bounds. Of course, if a failure does occur during this monitoring, the ability to predict (and prevent) that failure mode in future is greatly enhanced by that experience [21].

Because years of data collection of multiple units would be necessary to achieve statistically reliable failure data, the Arrhenius model is often used. An array of parts is age-accelerated by elevated temperature, and then the failure data is scaled back to the actual operating temperature. These data are then statistically combined using the data and techniques of MIL-HDBK-217F. The actual intent of MIL-HDBK-217F was as a design tool, not a prediction tool, allowing designers to trade off various designs (high reliability parts vs. normal parts, designs with lower parts counts, etc.). The use of this data for predictive purposes is not very valid, but often is used regardless, largely because there has yet to be discovered a good predictive model [22]. This is not surprising since electronic systems are made up of so many diverse parts, and there are so many manufacturing variables, such as soldering quality, handling, storage, that are not able to be evaluated from the MIL-HDBK model . Some of the concerns about attempting to apply MIL-HDBK-217 include:

- The handbook's reliability predictions pertain only to the 'flat' part of the bathtub curve, and there is no ready agreement on where the flat part of the curve is for electronic systems. In fact the bathtub curve, which works well for incandescent lightbulbs, may be a poor understanding of a system made up of hundreds of diverse parts, even if one were to assume that each of these parts was operating on a bathtub curve of its own [23].
- The above is one reason that these empirical reliability predictions typically correlate poorly to actual field performance [23].
- Since the models are based upon industry wide average failure rates, differences between manufacturers and the quality of their processes are not considered [23].
- This approach overly credits the Arrhenius model for failure modes (the Arrhenius model is really limited to those individual failure modes where temperature can be a catalyst). It is well-known that other factors greatly affect electronics reliability – dust and moisture contamination, power cycling, and vibration to name just a few [22]. Since these factors are so significant in the reliability of the part, models that fail to include these are inherently flawed.
- The Arrhenius model is derived from organic insulation degradation which is in fact well modeled by Arrhenius. But although insulation failure, for example increased leakage through an insulating package, can cause a failure, it is not an important mechanism compared to others. Accepted data indicates that at least 78% of electronic failures are due to other issues such as: design errors, PCB assembly defects, solder and wiring interconnect failures, PCB insulation resistance and via failures, dust, temperature cycling and software errors, etc. [23].
- The model makes the gross assumption that all "identical" assemblies/components are expected to have the same reliability. This is can be a poor assumption because of variations in manufacturing lots, temperature profiles in the hosting cabinet, differences in how the boards are used (normally driving current or normally off) etc [22].

- Although appearing quantitative, significant judgment is needed to establish a reasonable inspection or replacement interval. This judgment must also include consideration of the actual design of the replacement board. For example, military grade ceramic integrated circuits found in older equipment may actually be more reliable than plastic packaged parts that are designed for the consumer market with the attendant shorter life expectancy [22].
- The method does not include real data collected on operating I&C boards [22].
- The probability of failure produced applies to a grouped average of boards with similar characteristics to the one considered for evaluation [22].

If reliability models are not used, then the default is to replace the circuit board on a periodic schedule for replacement before failure is expected to occur, or to wait until the I&C board failure is discovered by periodic testing, spurious trip, or failure to activate a system when needed [22].

If one cannot use reliability models to predict the failure of a circuit board, there exist four possible approaches:

1) Guess at a useful life (or use observed failure data) and replace the boards before failure rates soar
2) Periodically remove the board from the equipment and test it on the bench. If this is done, key parameters for that board should be noted and trended.
3) Leave the board in place and use built in test equipment to verify its operation. This approach is based on the observation that handling older circuit boards greatly increases the risk of failure due to mechanical stresses and insertion-withdrawal cycling
4) Find some way to trend the board's key parameters while in the equipment

Predictive Maintenance

Predictive maintenance can be defined as follows: the process of using measurements to detect the onset of system degradation, thus permitting the elimination or mitigation of causal stressors prior to any significant deterioration in the component physical state. These measurements can be used to determine current functionality and ascertain future functional capability [20].

The basic difference between predictive maintenance and preventive maintenance is that predictive maintenance is based on actual measured conditions, rather than simply inferring deterioration on some preset schedule [20]. As discussed above, the determination of that preset schedule is fraught with uncertainty and guesswork.

Predictive maintenance is also known as condition monitoring or predictive testing and inspection. It uses primarily non-intrusive testing techniques, visual inspection and performance data to determine the condition of the system. Rather than basing actions on arbitrarily timed maintenance tasks, it initiates maintenance that is performed only when warranted by equipment condition. This approach of continuous analysis of equipment condition data allows the identification of incipient failures and can thus allow for planning and scheduling of maintenance or repairs before an actual functional failure would take place [21].

Following are the ways that predictive maintenance data is collected and used to determine the condition of the equipment to identify the precursors of failure [21]:

- Trend analysis – a key parameter is measured periodically and the results analyzed to detect a degradation process [21].
- Pattern recognition - the behavior of equipment, or combinations of parameters derived from the equipment is used to identify departure from normal operation [21].
- Data comparison – For example, information derived from other sources (e.g. other channels or other types of instruments) is compared with the system's data [21].
- Tests against limits and ranges – a value is observed and compared against what would normally be expected [21].
- Correlation of multiple technologies – similar to data analysis above, this approach allows for a diversity-based comparison [21].
- Statistical process analysis – Data is collected and statistically analyzed for deterioration [21].

While preventive maintenance is very powerful, it does not lend itself to all types of equipment, situations and failure modes. A circumspect approach to determining maintenance type must be used to allow for the wide range of system failures that might occur [21].

Prognostics are processes by which potential failures are identified in advance before the system is degraded or fails. By the use of prognostic information, appropriate maintenance activities can be scheduled. There have been several studies that have proposed applying prognostic techniques to electronic devices and systems. These include discrete electrical components such as FETs, printed circuit boards and even enterprise servers [4].

There are three broad approaches to applying prognostics techniques to electronics systems [4]:

1) Using expendable prognostic cells [4].
2) Monitoring and reasoning of parameters (such as shift in performance parameters, progression of defects) [4].
3) Modeling stress and damage in electronics utilizing exposure conditions coupled with physics-of failure [4].

One approach is to treat the product as a "black box". In black box testing, the premise is that it is not necessary to understand the workings inside the product; rather, data taken from the output signals is applied to an algorithm that is used to identify the failure precursor. This algorithm is "trained" on what to expect over a wide range of operating conditions. While attractive in theory, this approach is difficult to implement in its purest sense, since the system under test is subject to environmental changes that might affect its output performance. The algorithm then would have to be trained for the range of temperatures over which the equipment would need to operate. It is likely that actual failures would have to be encountered so that the algorithm could be instructed on what to look for to trigger an alert. Since there are many failure mechanisms possible in a complex system, the time that the equipment would be "in training" may be very long to acquire a reasonably complete failure mechanism array. It has the real and serious drawback that if failure modes are not uncovered during training, the algorithm would miss these faults and fail to do the prognostic alert [4].

Although problematic, method 2 may be the most promising of the three categories discussed above for the nuclear power industry. Method 1 requires designed-in considerations, while method 3 requires detailed knowledge of failure modes. Method 3 is not much value for complex electronic assemblies or systems, since the number of failure modes for the equipment is very large, but it may work well on single components.

Prognostic methods have been studied with respect to use on electronic products (see Table 2 of Reference [4]). Some examples of precursor methods are:

- Power supplies being monitored for power efficiency and output voltage (this is a very common practice already within the nuclear power industry) [4].
- Temperature sensors embedded in notebook and desktop computer using temperatures (CPU, motherboard, hard disk) [4].
- Computer servers in which using currents, voltages, temperatures and bit error rates are monitored [4].

Some common parameters that have been used as potential failure precursors for certain classes of electronics include [24]:

Switching Power Supply [24]

- DC output (voltage and current levels) [24]
- Ripple [24]
- Pulse width duty cycle [24]
- Efficiency [24]
- Feedback (voltage and current) [24]
- Leakage current [24]
- RF Noise [24]

Cable and Connectors [24]

- Impedance changes [24]
- Physical damage [24]
- High-energy dielectric breakdown [24]

RF power amplifier [24]

- Voltage standing wave ratio [24]
- Power dissipation [24]
- Leakage current [24]

Note that this list does not include much experience on digital systems. This is because the complexity of these systems makes the failure modes varied and the points that can be monitored extremely large. While reliability issues are driving the replacement of existing old systems in nuclear power plants, it is interesting to note that some modern digital electronics are less reliable due to their complexity and size [6].

The concept of predictive maintenance for electronics is very attractive. In many cases, carefully thought-out predictive maintenance techniques and plans can lead to reduced failures. It is however, by no means, a panacea. As equipment gets more complex, the ability to identify and monitor precursor parameters for incipient failures becomes essentially impossible because of the number of nodes and intermediate signals, which are often bit streams, involved. Basing a predictive maintenance regimen on an incomplete analysis of potential failure modes is very risky, since there would be a false sense of security that the equipment is being monitored, but in fact it may be degrading in a way that was not identified as a failure mechanism, Again, this probability increases dramatically as the system complexity increases. However, where predictive techniques can be reasonably applied, predictive maintenance may prove more economical than preventive maintenance. In this case, periodic maintenance that replaces equipment that is not near failure, based solely on a time interval can be wasteful and brings risks that come with any maintenance procedure.

The best approach is to derive a plan based on what is known or can be known about the failure modes of the system and where the “weak” points are. Devise non intrusive ways to measure the parameters of concern and determine what levels of variation indicate problems. This comes only with experience with the equipment or consultation with other users, or in some cases, the original manufacturer. One of the best places to start is the failure records of the equipment. If there are chronic problems or recurrent failures, some effort must be expended to determine the causes and what parameters are likely to indicate that the particular devise.

Features Provided By Equipment Manufactures to Assist with Maintenance

Many digital equipment manufacturers provide built-in tests, monitoring and diagnostic features with their equipment. These features assist in the proper maintenance and operation of the equipment.

Some examples are:

Self-tests / self-diagnostics

Many manufacturers include offline and/or online diagnostics. On-line diagnostics are typically configured to run continuously and alert the user if a diagnostic test fails. Some systems have off-line, user-initiated diagnostic tests which typically provide more detailed information to the system maintainer than the on-line tests.

Data Logging

Advanced logging systems store operating conditions and parameters. This data can be used to track failures or degradations over time to permit trending by the maintainer. Additionally, this data can be used to understand the events that lead to a failure of the system to assist with corrective actions.

Local Indicators and Failure Alarms

These features alert the operators of the equipment to the different equipment failures and often the severity of the failures. Such indicators help pinpoint the location of the failed component or module [2].

Keying and Interlock Features

Features such as keying (electronic and physical) and modular construction facilitate the correct replacement of components. Interlocks prevent incorrect configurations and enhance personnel and equipment safety by preventing unsafe maintenance actions.

Hot-swap features

Hot-swap features enable rapid maintenance and uninterrupted operation of the equipment during the maintenance activity [2].

Auto-calibration / test features

These features permit system and system interface calibration without requiring detailed interaction between the system maintainer and the equipment [2].

Preventive Maintenance Performed by the Nuclear Power Industry

To determine the preventive maintenance being performed within the nuclear power industry several sources were examined. Applicable EPRI reports were examined (see references [2] and [3]) and a search of documents on the internet and the Institute of Electrical and Electronics Engineers (IEEE) Xplore database was performed. A large portion of the publicly available information focuses on failures of digital I&C systems and obsolescence issues (e.g. see references [5][6][19]).

One of the more recent documents published by EPRI, "Digital Control Systems: Survey of Current Preventive Maintenance Practices and Experience" [3], provides a discussion of the current practices within the industry. Some of the key findings are:

"Most existing PM activities for systems that have been upgraded to DCSs [Distributed Control Systems] are based on the previous analog system PM requirements, PM requirements for analog components that interface with the DCS, and to a lesser extent the PM requirements of the installed DCS components." [3]

"DCS vendors seldom provide PM recommendations for DCSs, other than specific DCS software and logic checks. In general, when PM recommendations are provided, there are fewer PM requirements with DCSs than with a comparable analog system." [3]

"Some routine DCS and associated analog component conditioning monitoring (CM) is performed. The majority of the CM utilizes techniques employed in analog systems. Thermal and vibration surveys and visual inspections are performed on critical panels at some plants. DCS monitoring and trending capabilities are useful in performing on-line CM." [3]

"DCS monitoring and trending capabilities are useful in performing on-line CM." [3]

In order to supplement the literature search, a series of phone interviews of plant and utility personnel was conducted to learn about the types of preventive maintenance being performed throughout the industry. The questions that were asked of each person are given below:

1) What kind of preventive maintenance (preventive or predictive) do you perform on your digital systems (battery replacement, power supply replacement, periodic reboots, etc.)?
    a) Do you have any good practices to recommend (avoid power cycling, avoid thermal cycling, use training hardware to test-out maintenance activity, etc.)?
    b) Do you have any stories of failures that led to new maintenance?
    c) Have you had any issues with version/revision control (software or hardware)?
    d) Have you had any issues with constants/parameters after replacement of failed modules?
    e) Do you perform any maintenance based on performance trending (power supply voltage ripple, processor timing, etc.)?
2) What kind of training is required of the personnel who maintain the equipment?
    a) Do the technicians working on the equipment receive any specialized training (vendor or utility-provided)?
    b) Are all technicians qualified to work on digital systems, or is there a subset who has received specialized training?
    c) If specialized training is provided, what high-level topics are covered?
3) Do you perform any kind of tin whisker mitigation activities for the equipment?

Approximately 50 people familiar with digital I&C systems in the nuclear power industry were contacted for this report. This group was composed of persons both from utility corporate and plant staff with either key engineering or maintenance roles for their respective organizations. The responses were collected in an Excel spreadsheet and analyzed and sorted into two categories: Maintenance Activities and Maintenance Practices. Maintenance Activities are the actions that are performed on the equipment and Maintenance Practices include considerations or the philosophy behind generating and executing a maintenance program. The Maintenance Practices category includes items like "ensure adequate quantities of spare modules and parts are available due to fast obsolescence" or "utilize built-in self tests and diagnostics of equipment". Since many of the responses were the nearly the same, a set of "generic" Maintenance Activities and Maintenance Practices were generated from all of the collected data.

Each of these Maintenance Activities was classified as one of the three types of maintenance discussed in Section 1: Reactive, Preventive or Predictive Maintenance. This data is presented in Table 3-1. Note that it is possible for a particular maintenance activity to be part of more than one type of maintenance strategy. For example, by checking system logs periodically, the data can be used to determine that a component has failed and needs replacement (Reactive Maintenance), that a component has been operating for a certain number of hours and should be replaced (Preventive Maintenance) or that a parameter associated with a component is trending in a negative direction indicating possible future failure (Predictive Maintenance). Examining the data in Table 3-1, it is seen that a majority of the maintenance practices collected via the interviews are preventive in nature. This is not surprising since experience with non-digital systems, particularly mechanical systems such as pumps and valves, demonstrates that failure rates and mean-time-between-failures are often well known and preventive maintenance can be particularly effective for these systems. So it is therefore logical, that maintainers would adopt the same maintenance approach in the absence of any information instructing them to do otherwise.

Similar information from other industries and digital instrumentation and control owners/users outside of the nuclear power industry was collected through the same interview process. This was done to discover if there were any maintenance practices that are being performed outside of the nuclear power industry that have applicability to the nuclear system owners and maintainers. Interviews were conducted with personnel familiar with the maintenance of both shipboard machinery controls and RADAR, communication and data systems. Like the data from the nuclear power industry respondents, most of the activities collected were similar between respondents so a set of generic activities was generated. Table 3-1 shows a list of these maintenance activities and the type of maintenance that they may be considered. Additionally, the table notes if that activity is also performed in the nuclear power industry. Almost all of the activities identified by the non-nuclear power industry respondents are also being performed by the nuclear power industry interviewees. The only exception is that of "Check network latency for each processor". This of course, is not to say that it is not being done by certain utilities or plants, just that none of the nuclear power industry respondents for this paper indicated this activity. The good agreement between the nuclear power industry and shipboard systems is encouraging and suggests between the two that perhaps the proper set of maintenance activities are being performed.

Arguably, the most fundamental reason that routine maintenance is performed on digital instrumentation and control systems is to ensure the continued operation of the system. The typical philosophy is to ensure that the preventive maintenance program will prevent hardware failures. This is perfectly consistent with the data presented in Section 2 where Hardware Failure is listed as one of the primary causes of digital system failures. However, it is worthwhile to examine if the present maintenance practices address any or all of the other types of failure presented in Section 2 in addition to hardware failure. This is especially important, as some of the other types listed are significant sources of digital failure (particularly human performance). It seems reasonable that a system owner should attempt to mitigate the possibility of as many of the failure types as possible to ensure continued operation of the equipment. With this premise in mind, a comparison was performed between the various maintenance activities provided by the survey respondents against the reasons for digital failures presented in Section 2. Table 3-2 shows each maintenance activity and the particular digital failure that it has the potential to mitigate. The blue boxes indicate that the activity has the potential to reduce the likelihood of that type of digital failure from occurring. The green boxes indicate that at least one respondent indicated that their maintenance procedures include an activity that diminishes the possibility of that particular failure type.

Note that the categories of Ineffective Change Management / Process, Human Performance, Inadequate Training and Inadequate Operating Procedures do not have any boxes highlighted as none of the activities appear to address these categories. The absence of these highlighted boxes is significant, as Human Performance and Ineffective Change Management/Process are the first and fifth most prevalent types of digital system failures. Further effort should be expended to explore if maintenance activities could be altered or enhanced to address issues related to these categories.

Table 3-1
Maintenance Activity vs. Type of Maintenance

Generic Maintenance Activities (Nuclear Industry)	*Reactive*	*Preventive*	*Predictive*	*Performed on Shipboard Systems*
Audit configuration periodically		X		
Calibrate equipment periodically		X		X
Check redundancy functions for power supplies and CPUs periodically	X	X		X
Check system logs periodically	X	X	X	
Clean and inspect cabinets / equipment periodically	X	X		X
Clean and inspect fans / filters periodically		X		X
Inspect cabinets / equipment periodically	X	X		X
Monitor each individual power supply of redundant or auctioneered arrangements	X	X	X	
Monitor use of system resources	X	X	X	
Perform functional test of system periodically	X	X		
Perform TDRs of fiber optic communication links periodically	X	X	X	
Perform thermal scan of processors / circuit cards periodically	X	X	X	
Power-down HMIs periodically		X		X
Power-down processor-based systems periodically		X		X
Remove log files periodically		X		X
Replace batteries periodically		X		X
Replace circuit cards periodically		X		
Replace clock chips periodically		X		
Replace electrolytic capacitors on backplanes and circuit boards periodically		X		
Replace fuses periodically*		X		
Replace HMI hard drives periodically		X		
Replace HMI VRAM batteries periodically		X		
Replace LCD monitors periodically		X		X
Replace NOVRAM periodically*		X		
Replace power supplies periodically		X		
Replace relays periodically*		X		
Replace VRAM batteries periodically		X		X
Replace workstations periodically*		X		
Scan electromagnetic emissions of cabinet periodically	X	X		
Scan for viruses periodically		X		
Swap active and standby power supplies periodically	X	X		
Synchronize clocks on digital systems if not connected to a common time source periodically		X		
Test batteries periodically		X		
Tighten terminal connections periodically*		X		
Trend computer system / DCS processing time		X	X	X
Trend critical parameters		X	X	
Trend how often equipment "locks-up"		X	X	
Trend power supply voltage and ripple to detect degradation		X	X	X

Generic Maintenance Activities (Shipboard Systems)	*Reactive*	*Preventive*	*Predictive*	*Performed in Nuclear Industry*
Clean and inspect fans / filters periodically	X	X		X
Replace VRAM batteries periodically		X		X
Clean and inspect cabinets / equipment periodically	X	X		X
Calibrate equipment periodically	X	X		X
Perform functional test of system periodically	X	X		X
Trend computer system / DCS processing time	X	X	X	X
Check network latency for each processor	X	X	X	
Replace batteries periodically		X		X
Power-down processor-based systems periodically		X		X
Remove log files periodically		X		X
Trend power supply voltage and crystal currents to detect degradation		X	X	X

* Data from EPRI Report 1022713

Table 3-2
Maintenance Activity vs. Type of Digital Failure That It May Mitigate

Generic Maintenance Activities	*Hardware Failure*	*Inadequate SW Design*	*Inadequate HW Design*	*Inadequate Testing*	*Ineffective Configuration Management*	*Ineffective Change Management / Process*	*Human Performance*	*Inadequate Training (includes simulator issues)*	*Inadequate Maintenance Procedures*	*Inadequate Operating Procedures*	*Inadequate Vendor Information / Oversight*	*Inadequate Software V&V*	*Manufacturing Defect*	*Inadequate HMI Design*
Audit configuration periodically	X				X									
Calibrate equipment periodically	X				X						X	X		
Check redundancy functions for power supplies and CPUs periodically	X			X					X				X	
Check system logs periodically	X	X	X	X	X				X				X	
Clean and inspect cabinets / equipment periodically	X			X										
Clean and inspect fans / filters periodically	X			X										
Inspect cabinets / equipment periodically	X			X										
Monitor each individual power supply of redundant or auctioneered arrangements	X		X	X					X				X	
Monitor use of system resources	X		X	X					X				X	
Perform functional test of system periodically	X	X	X	X					X				X	X
Perform TDRs of fiber optic communication links periodically	X	X	X	X					X				X	
Perform thermal scan of processors / circuit cards periodically	X		X	X					X				X	
Power-down HMIs periodically	X	X		X								X		X
Power-down processor-based systems periodically	X	X										X		X
Remove log files periodically	X	X	X									X		
Replace batteries periodically	X			X					X				X	
Replace circuit cards periodically	X		X	X	X				X				X	
Replace clock chips periodically	X			X					X				X	
Replace electrolytic capacitors on backplanes and circuit boards periodically	X			X					X				X	
Replace fuses periodically*	X			X					X				X	
Replace HMI hard drives periodically	X			X					X				X	X
Replace HMI VRAM batteries periodically	X			X					X				X	X
Replace LCD monitors periodically	X		X	X					X				X	X
Replace NOVRAM periodically*	X			X					X				X	
Replace power supplies periodically	X		X	X	X				X				X	
Replace relays periodically*	X			X					X				X	
Replace VRAM batteries periodically	X			X					X				X	
Replace workstations periodically*	X			X					X				X	
Scan electromagnetic emissions of cabinet periodically	X		X	X									X	
Scan for viruses periodically	X	X										X		
Swap active and standby power supplies periodically	X			X					X				X	
Synchronize clocks on digital systems if not connected to a common time source periodically		X										X		
Test batteries periodically	X			X					X				X	
Tighten terminal connections periodically*	X			X					X					
Trend computer system / DCS processing time	X	X	X	X					X				X	
Trend critical parameters	X		X	X					X					
Trend how often equipment "locks-up"	X	X	X	X					X				X	
Trend power supply voltage and ripple to detect degradation	X		X	X					X				X	

* Data from EPRI Report 1022713

This data shows that almost all reported maintenance activities are designed to prevent hardware failure. There appears to be good "coverage" for the failure types of Inadequate Hardware Design, Inadequate Testing, Inadequate Maintenance Procedures, Manufacturing Defects and Inadequate HMI Design. There are several activities listed that may mitigate failures attributable to Inadequate Software Design. As mentioned earlier, maintenance activities are not normally designed to detect software design issues. However, there are instances where operating conditions of the system may have changed from the time the system was designed and its software tested. One example is the presence of a vulnerability in the system software that was not known at the time of its creation and so was not detected by any vendor or end-user tests. Performing a periodic virus scan on this system may detect a virus designed to exploit this vulnerability before it causes a failure.

The data table also shows that there is little or no coverage for Ineffective Configuration Management, Ineffective Change Management / Process, Human Performance, Inadequate Training, Inadequate Operating Procedures, and Inadequate Vendor Information / Oversight.

It is important to understand that the table data is largely qualitative in nature as it is based on personal interviews of a finite set of nuclear power industry digital system owners. Additionally, there is some judgment needed to determine whether a particular activity impacts the possibility of a digital failure type. The purpose of this table is to provide an indication to the system owner about how broad reaching each maintenance activity is regarding digital failure type. It is important to remember that some of the digital failure types are mitigated by other plant processes (e.g. design change process), so the table is not meant to convey that digital failure types without a blue or green box are not being addressed by system owners or maintainers.

Even though there may be other plant processes in place to handle most if not all of the digital system failure types, the data highlights that routine maintenance provides an opportunity to further mitigate these digital failures. As an example, one respondent reported the following for their "Replace power supplies periodically maintenance activity":

"Power supply boards and other boards are replaced by PM events, and configuration of the new device set up to match the original device being replaced (dip switch settings, firmware revision). Then configuration control documentation is reviewed to ensure that the part being installed (configuration) matches the controlling documentation. Discrepancies are investigated."

Not only does this activity cover against hardware failure (replacing a power supply before it fails), but checking the configuration helps address the "Ineffective Configuration Management" failure type as it provides an additional verification against the proper configuration of the system.

Consider a second example from the survey concerning the "Perform functional test of the system periodically":

"We have a switchyard that is operated by two systems: our DCS and the power line operator. Following installation of the DCS, periodic testing of breaker 'reclosure' function (recloses following a lightning strike or temporary fault) identified a condition where our DCS is blocking this reclosure function. Our risk of a loss of offsite power is increased by this condition. Redesign of the logic is being planned."

Here, we see that the test was able to detect a defect in the software ("Inadequate Software Design"). However, as discussed before about using maintenance to detect software defects, this was largely a chance discovery.

As one last example, some utilities perform thermal scans of their equipment ("Perform thermal scan of processors / circuit cards periodically") to determine if the equipment is running too hot or if operating temperatures are trending up. Not only does this indicate a possible problem with a particular piece of hardware, but it could detect "Inadequate Hardware Design" if the equipment is operating correctly but the vendor failed to design-in sufficient cooling for the cabinet. Of course, any design inadequacy should have been detected during initial testing.

It is good to point out here, that in all cases system owners rely on other processes, such as the design change process to catch the kinds of errors discussed above as often there will be a great deal of scrutiny and testing of a new system before its installation. However, one can see that by employing certain procedures or maintenance activities, an opportunity is available to detect errors that were missed by other processes.

In Section 2 the stressors that contribute to the failure of electronics were listed. It is worthwhile to examine the list of maintenance activities obtained from the interviews to see if they reduce (or have the potential) to reduce any of the known stressors for electronic devices. Table 3-3 provides this data. Atmospheric Pressure and Cosmic Rays have been grayed-out because neither has been found in the literature to contribute significantly to failures of electronics in ground-level systems. One notable exception is that systems that contain high-voltage semiconductors operating at high voltages have been found to be subject to higher failure rates due to cosmic radiation [25][26] .

We can see in Table 3-3, that a majority of the preventive maintenance activities collected do not address the stressors for electronics. Like the data presented in Table 3-2, this chart is presenting qualitative information about activities discovered via interviews. It is not intended to convey that system owners are not doing enough to reduce the stressors for electronics. The purpose of this data is to highlight that certain preventive maintenance activities reduce (or have the potential) to reduce stressors for digital electronics. Again, the reduction of these stressors may be handled by other plant processes especially during the design phases of the systems (e.g. locating certain cabinets in an air-conditioned space to reduce thermal stresses).

Table 3-3
Maintenance Practice vs. Stressor of Electronic Devices

Generic Maintenance Activities	*Thermal*	*Electrical*	*Mechanical*	*EMI*	*Humidity*	*Salinity*	*ESD*
Audit configuration periodically							
Calibrate equipment periodically	X	X	X	X			
Check redundancy functions for power supplies and CPUs periodically							
Check system logs periodically							
Clean and inspect cabinets / equipment periodically	X	X	X	X	X	X	X
Clean and inspect fans / filters periodically	X		X		X	X	
Inspect cabinets / equipment periodically							
Monitor each individual power supply of redundant or auctioneered arrangements							
Monitor use of system resources							
Perform full functional test of system periodically							
Perform TDRs of fiber optic communication links periodically							
Perform thermal scan of processors / circuit cards periodically							
Power-down HMIs periodically							
Power-down processor-based systems periodically							
Remove log files periodically							
Replace batteries periodically							
Replace circuit cards periodically		X		X			
Replace clock chips periodically							
Replace electrolytic capacitors on backplanes and circuit boards periodically		X		X			
Replace fuses periodically*		X		X			
Replace HMI hard drives periodically							
Replace LCD monitors periodically							
Replace NOVRAM periodically*							
Replace power supplies periodically	X	X		X			
Replace relays periodically*		X		X			
Replace VRAM batteries periodically		X					
Replace workstations periodically*							
Scan electromagnetic emissions of cabinet periodically							
Scan for viruses periodically							
Swap active and standby power supplies periodically	X	X		X			
Synchronize clocks on digital systems if not connected to a common time source periodically							
Test batteries periodically							
Tighten terminal connections periodically*	X	X	X	X			
Trend computer system / DCS processing time							
Trend critical parameters							
Trend how often equipment "locks-up"							
Trend power supply voltage and ripple to detect degradation							

* Data from EPRI Report 1022713

So far, we have only considered the preventive maintenance activities and how they compare against the failure types and stressors for digital electronics. The same analyses can be performed for the maintenance practices that were collected from the interviews. The list of obtained preventive maintenance practices vs. digital failure type is shown in Table 3-4. Scanning the table, it can be seen that there is fairly good coverage of many of the failure types. The digital failure types that seem to have the least coverage are Inadequate Software Design, Inadequate Hardware Design, Configuration Management, Ineffective Change Management / Process, Inadequate Operating Procedures, Inadequate Vendor Information / Oversight, Inadequate Software V&V and Inadequate HMI Design. Like the data for maintenance activities presented in Table 3-2 and Table 3-3 all of these categories are handled by other plant process, so the chart is not mean to construe that the utilities are not addressing these issues elsewhere. Indeed, maintenance may reveal problems in these areas, but it should not be used as the primary method to address them. These are far better addressed with design, verification and validation tests and plant processes. The point here is that maintenance in some cases may provide a way to detect issues that were missed or unanticipated by other processes and activities. A similar recommendation is made regarding the results of the comparison of the maintenance practices vs. digital failure types as that of the maintenance activities vs. digital failure types. That is, to the maximum extent feasible, system maintainers should incorporate into their maintenance programs and philosophy ways and methods to reduce the possibility of occurrence of as many of the digital failure types as possible.

Table 3-4
Maintenance Practice vs. Digital Failure Type

Generic Maintenance Practices (Nuclear Industry)	Hardware Failure	Inadequate SW Design	Inadequate HW Design	Inadequate Testing	Ineffective Configuration Management	Ineffective Change Management / Process	Human Performance	Inadequate Training (includes simulator issues)	Inadequate Maintenance Procedures	Inadequate Operating Procedures	Inadequate Vendor Information/ Oversight	Inadequate Software V&V	Manufacturing Defect	Inadequate HMI Design
Be cognizant of shelf-life of replacement parts														
Be cognizant that not all of vendor's recommend PM may be able to be perform (not able to shut down equipment)														
Be cognizant that vendor may include more built-in diagnostic alarms than industry desires (nuisance alarms)														
Consider cyber security as part of PM	X	X										X		
Create custom logging for plant specific information	X	X	X	X					X				X	
Create PM templates based on vendor recommendations, environmental conditions and operating experience	X			X					X		X			
Design systems to be single-failure tolerant to permit reactive maintenance strategy		X	X	X			X	X	X			X	X	
Ensure adequate quantities of spare modules and parts are available due to fast obsolescence														
Ensure PM procedures are consistent with vendor recommendations.	X			X				X					X	
Generate digital modification standard that covers lifecycle of digital upgrades	X	X	X	X	X	X	X	X	X		X	X	X	X
Implement digital upgrades/replacements in stages	X			X	X	X		X	X		X	X	X	X
Implement qualification program to ensure maintainers have correct training to service equipment							X	X	X					
Inspect replacement circuit cards before installing	X												X	
Limit exposure to high temperatures														
Limit power cycling of cabinets, particularly during outages	X	X	X						X				X	
Minimize human interaction with equipment							X	X						
Obtain maintenance training from vendor							X	X	X					
Perform burn-in of replacement parts before installing														
Photograph and archive photos of new circuit cards - use this for future inspections	X	X	X	X					X				X	
Plan small upgrades to handle obsolescence issues	X			X	X	X		X	X		X	X	X	X
PM should be tailored to environment that equipment is operating in	X			X					X		X			
Provide training on circuit cards, power supplies, detectors/sensors							X	X	X					
Provide training tailored to system							X	X	X					
Purchase extra system, particularly up front, to use for training and trying out fixes, patches, upgrades, etc.							X	X	X	X	X	X		
Review vendor's patch list before installing		X										X		
Store parameters for devices and keep copies in separate place					X		X		X					
Supervise vendor maintenance in order to maintain configuration control	X				X									
Understand the metrics and surveillance that the system runs	X			X			X	X	X				X	
Use AP 9.13 to as a guide to what maintenance should be performed	X			X				X	X				X	
Use subject matter experts to assist with training							X	X	X					
Utilize built-in self tests and diagnostics of equipment	X			X			X	X					X	

Generic Maintenance Practices (Shipboard Systems)	Hardware Failure	Inadequate SW Design	Inadequate HW Design	Inadequate Testing	Ineffective Configuration Management	Ineffective Change Management / Process	Human Performance	Inadequate Training (includes simulator issues)	Inadequate Maintenance Procedures	Inadequate Operating Procedures	Inadequate Vendor Information/ Oversight	Inadequate Software V&V	Manufacturing Defect	Inadequate HMI Design
Clean fans, perform disk checks, etc. on computer/server equipment that support PLCs	X			X										
Obtain specific training from the company who integrated the system							X	X	X					
Place configuration files under configuration management after grooming system					X		X		X					

Effectiveness of Preventive Maintenance Activities

Determining the effectiveness of the preventive maintenance practices employed by the nuclear power industry has proved to be a difficult task. This is due to the relatively small number of installed systems, use of several manufacturer's equipment and lack of or disparate methods used by the equipment owners and maintainers in tracking digital failures and causes.

An attempt was made to evaluate the effectiveness of the current activities using the LER and INPO data analyzed in Section 2. The data was examined to see if (percentage-wise) the occurrences for each failure type have remained the same or changed within the past few years. This may give a rough idea of the impact of maintenance activities. Admittedly, many other processes (in addition to maintenance) impact these categories. However this data may yield insight into what areas maintenance activities should be targeted.

The percentage of each type of failure of the total number of failure types recorded for the data from the previous study and data from LERs and INPO data covering the 2008-2012 time span were generated. The data for each of these sets is shown in Figure 3-1. It is apparent that the two data sets differ appreciably. The types that have seen a 5% or greater increase are Inadequate Maintenance Procedures, Inadequate Vendor Information / Oversight and Ineffective Change Management / Process. These results may simply indicate that there have been an increase in the number of new installations and not necessarily a negative trend in the process and procedures used.

Only a single type saw a 5% or greater decrease (Inadequate Hardware Design). This result may indicate that the equipment is very reliable and perhaps is becoming more reliable.

The highest percentages of digital failure types are Human Performance, Hardware Failures, Inadequate Software Design, Inadequate Maintenance Procedures and Inadequate Vendor Information / Oversight. This result is not necessarily discouraging because Hardware Failure percentage has decreased and the categories of Human Performance, Inadequate Maintenance Procedures and Inadequate Vendor Information / Oversight can be overcome not with complicated or exotic maintenance processes or methods but through improved plant processes, procedures and oversight.

Single Point Vulnerability and Manufacturing Defect disappeared completely as a digital failure type within the 2008 – 2012 timeframe.

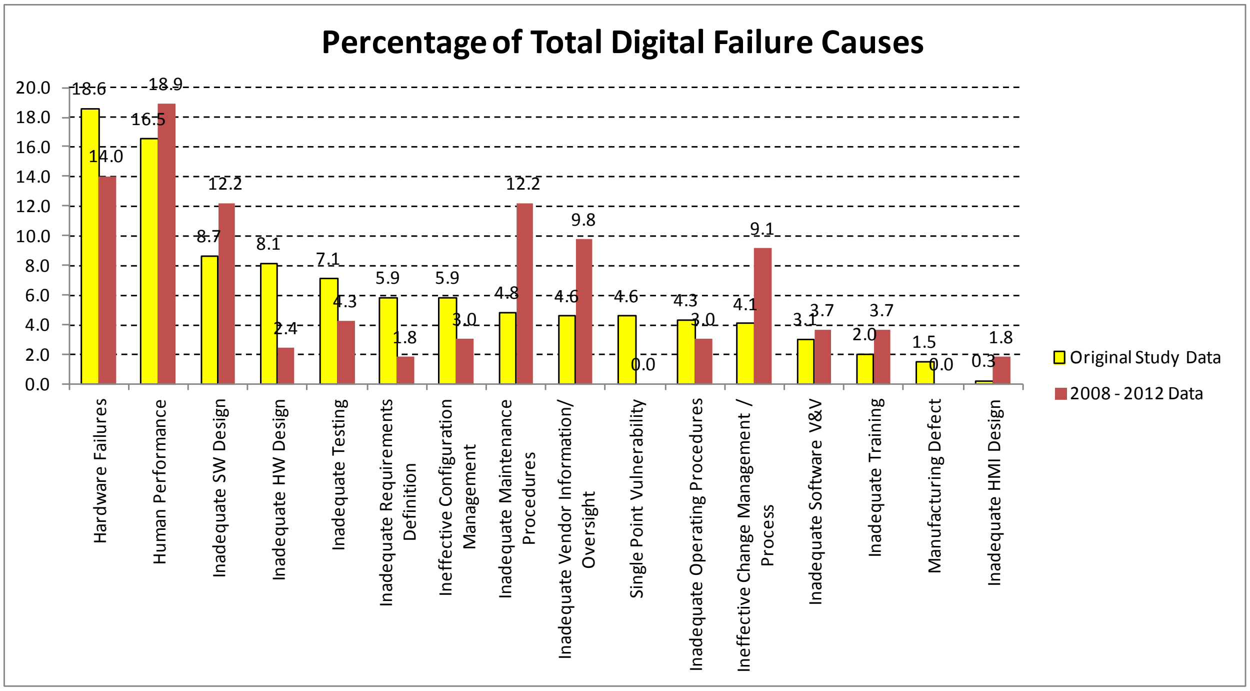

Figure 3-1
Comparison between Previous Study Data and Data from 2008-2012 (Percentages of Total Causes of Digital Failures)

4
RECOMMENDED PRACTICES

Digital systems may consist of processor cards, communication modules, digital interface modules, analog interface modules, relay cards, power supplies and other types of electronics. Several maintenance activities that are appropriate for analog circuitry and power supplies of analog I&C systems are also applicable to the same components within a digital I&C system. One of the great advantages of a digital I&C system in terms of maintenance is the enhanced ability to monitor and detect failures and incipient failures within system through manufacturer supplied built-in self diagnostics and monitoring software.

This section presents recommendations for preventive (and condition-based) maintenance for digital I&C systems within the nuclear power industry.

System-level Preventive Maintenance

System-Level Periodic Inspections

In-line with recommendations presented in [12], the scheduling of system-level inspections should be determined using these two criteria:

- The criticality of the system to nuclear safety
- The criticality of the system to power generation

Inspections of digital systems impacting nuclear safety should be conducted on their regularly scheduled surveillance interval as defined in the plant design basis documents. Non-safety related digital systems critical to the generation of electrical power should receive more frequent inspections. The intervals for inspection of this type of equipment should be based on the age of the equipment, environmental conditions the equipment is subject to the impact of a failure on plant operations and plant and industry operating experience for similar equipment.

Inspection of the digital I&C system should include:

1. Check the system and individual modules or card status lights to verify that the system is functioning correctly. Checking the status lights may provide indication of a failure that has not been reported to the user of the equipment.
2. Inspect for dust build-up on heatsink fins and clean if necessary. Note, do not use high pressure air to clean off dust from components.
3. Check for dirty or clogged air filters and clean or replace if necessary.
4. Ensure cooling fans (if equipped) are operating correctly. Listen for signs of worn fan bearings.

5. Verify that all circuit cards or modules are fully inserted into their respective chassis or backplane.
6. Visually inspect for damaged components, circuit cards and modules.
7. Inspect for loose connections (particularly the field wiring interfaces).
8. Look for smoky deposits or charred parts (particularly near power supplies and where higher voltages are present in the cabinet/chassis).
9. Check for arcing damage of fuses and fuse holders. Replace fuses as necessary.
10. Inspect sealed relays for discoloration or cracking.
11. Inspect backplane and printed circuit card / module connectors for cracking of the connectors, corrosion, oxidation, pin spreading [12] and metal whiskers. The insertion and removal of connectors causes wear on the connectors, connector housing and pins and sockets therefore, inspection should only be performed when during other activities it is necessary to disconnect the connectors.
12. Perform channel checks to verify that individual signals associated with the same plant parameter are within tolerance to each other.

Built-in Maintenance Software Tools

Almost all modern digital I&C systems contain self diagnostics to monitor for operational malfunctions or errors [2]. Many provide the capability to run diagnostic checks on the equipment through vendor supplied maintenance software. This is easily the most important tool that the system maintainer has at his or her disposal for proper maintenance of a digital I&C system.

The specific type and number of tests available will vary by manufacturer. These will typically consist of the following tests:

- Non-volatile Memory [2]
- Read-only Memory [2]
- Real Time Clock [2]
- RAM Check [2]
- Data Communications [2]
- Watchdog timer
- I/O (loop back, calibration)
- Power supply and internal bus voltages

These tests or a sub-set thereof are performed while the system is operating without impacting system functionality. Often a set of more in-depth tests are available when the system is offline. These tests may include the same set above, but executed to a greater degree and they may include tests targeted to the specific installed hardware of the digital system. Reference [2] provides a detailed discussion of the type of maintenance tests available to the maintainer for digital systems.

Where possible, one should maximize the use of automatically running on-line monitoring and diagnostic tools if it doesn't interfere with the proper operation of the system. In order for these tests to be effective, the maintainer should be properly trained on how to interpret the results or logs of any continuous tests being performed.

The frequency of this activity should be determined by considering the importance of the system to nuclear safety and/or power generation, manufacturer recommendations (or reliability data for individual hardware components), plant mode of operation and plant and industry operating experience.

Failure Detection

The types of failures that can be detected vary by manufacturer. The following is a list of failures that the software is typically designed to detect:

- Non-volatile memory failures [2]
- RAM failures [2]
- Watchdog timer timeouts (processor stall) [2]
- Communication failures (transmitters, receivers, loose or missing connections) [2]
- Power supply failures

Considerations

Ensure that administrative procedures are in-place and maintenance personnel are properly trained on the maintenance software to prevent inadvertent system disruption when initiating on-line tests or querying the system for the results of on-line tests.

For systems that are critical to nuclear safety or power generation, one should maximize the use of periodic off-line tests in-lieu of maintainer-initiated on-line tests to avoid the potential of human error induced system disruptions. However, simply querying the results of automatically running continuous tests has much less potential for inadvertent interference than a maintainer-initiated on-line test.

Utilize proper administrative controls to prevent malicious and inadvertent changes from being made to the digital platform. Configuration control must be maintained and verified during maintenance tool use.

When using the diagnostic tools, check system maintenance logs for non-alarmed faults.

It is important for the maintainer to know how to execute the test and how to properly interpret the information.

Many maintainer-initiated tests detect a failure (or multiple failures) that have already occurred but have not yet noticeably impacted the operation of the system as a whole. However, some of these tests can be used to detect incipient failures. Examples include trending network communication latency measurements or processor cycle times.

Redundancy Function Checks

Many digital I&C systems used in the nuclear power industry are based on an architecture containing redundant components. These systems typically are designed around a dual- or triple-redundant with some quad-redundant implementations being used for safety-related applications.

Dual-redundant Systems

Dual- redundancy may be implemented in a parallel structure where each component operates in conjunction with an identical component to provide identical functionality. The output of each redundant component is combined to provide a unified command or actuation. In these cases, where either component is capable of providing the function, failure of one component is sometimes not detected as there may be no interruption of system functionality. Therefore, control should be periodically switched from one redundant component to the other to ensure that both are operational. Note, that some manufacturer's equipment will automatically swap control between an active and standby module at regular intervals.

Other redundant schemes involve a fail-over architecture where one component is actively controlling or monitoring a process and the other is in a standby mode. In these systems, control should be periodically switched to the standby device to ensure that it is fully capable of providing the system functionality. It is also important to test the recovery back to the original device [2].

These activities should also be applied to systems with redundant power supplies or sources of power and communication modules/cards for the same reasons.

The frequency of this activity should be determined by considering the importance of the system to nuclear safety and/or power generation, manufacturer recommendations (or reliability data for individual hardware components), plant mode of operation and plant and industry operating experience. As an example, one manufacturer suggests that redundancy checks for its power supplies be performed either every 2 or every 5 years depending on the risk reduction factor sought by the owner/maintainer.

Failure Detection

This activity does not provide detection of an impending failure. Instead, it is used to ensure the continued availability of the system to perform its intended functions. It provides the capability to detect all failures of one of the redundant components within a redundant digital I&C system before that component is made an active component.

Considerations

It is possible that one of the redundant components of the system has already failed; therefore, it is best that this activity can be performed when the system is off-line.

Utilize system diagnostics to the maximum extent to ensure that the component about to assume the active role is fully functional.

Ensure that all redundant portions of the system are active/on before restoring the system to operation.

When performing this activity on power supplies, allow each power supply to supply the system for several minutes individually.

Ensure that there is positive and unambiguous indication of which component is the active one in the system to avoid placing the wrong component in service.

Triple-redundant Systems

Triple-redundant systems are implemented in a parallel structure where each component operates in conjunction with an identical component to provide the system functionality. Voting (usually 2-out-of-3) or averaging methods are used to determine responses to input signals. The major benefit of triple-redundant system is that maintenance can be performed on one of the redundant components without needing to take the system off-line.

Since a triplicated system requires only 2 of the 3 components to be operational for system functionality, it is not necessary to switch control over to a single component at a time to ensure continued functionality of the digital system. These systems perform self-tests on the redundant components and are able to identify when a single component "disagrees" with the other two.

Toggle Discrete Input and Output Signals

Often digital I&C systems maintain certain digital outputs at constant states during normal operation (trip output command, alarm contact, etc.). Additionally, many digital systems read digital values that remain constant during normal operation. It is important to verify that the digital system is capable of responding to (or changing the state of) a digital signal when needed. Many built-in diagnostics are usually limited to detecting continuity (wire breaks) and communication errors [2], although some systems provide the ability to detect stuck-on and stuck-off inputs and outputs. If the ability to toggle digital states is not provided as a built-in function of the maintenance software, this activity should be performed periodically to ensure the ability of the system to function as needed.

Failure Detection

Some examples of failures that these tests are designed to detect include:

- Stuck relay contacts
- Failed input buffer and/or associated circuitry (short or open circuit)
- Failed output driver and/or associated circuitry (short or open circuit)

Considerations

Ensure that administrative procedures are in-place and maintenance personnel are properly trained on the digital system and any maintenance tools to prevent inadvertent system disruption when toggling inputs and outputs.

Scan for Viruses

A fair number of events within the INPO database refer to instances where a computer virus was inadvertently introduced by a person performing a maintenance activity. It is therefore recommended that system owners / maintainers consider performing virus scans both before and after any maintenance activity involving a computer. This is recommended both for computer based digital I&C systems and any computer based test-tool or test equipment that interfaces directly with the digital I&C system. Additionally, one should scan any disks or portable memory devices before permitting them to be connected to the digital system.

Perform Functional or Application Level Test

For some digital I&C systems, the built-in tests and diagnostics may prove sufficient for an effective maintenance program. For systems that are critical to nuclear safety or power generation, system-level testing may provide additional confidence that the system is fully capable of performing its intended functions. These tests may be passive, where checks between redundant channels or known values are used or active, where test signals are injected into the system to verify capability [2]. Reference [2] goes into greater detail about the types and methods for application level testing for digital I&C systems and should be consulted when determining a maintenance strategy for digital systems.

Failure Detection

Application level tests have the ability to detect a variety of failures. These tests may expose issues with plant interfaces (and associated circuitry) with the digital I&C system, whereas the built-in tests are more likely to only detect failures of the digital system hardware.

Considerations

Active testing requires greater effort and complexity (especially if test fixtures or external equipment is needed) than passive testing. This testing should be kept as simple as possible and minimized due to its potential for system disruption.

Internal function tests often require implementing or initiating bypasses. Therefore, these tests should be manually initiated. Automated internal function active tests are recommended only if a means to automatically initiate bypasses is provided [2].

Some manufacturers provide tests that can verify some functionality of various output devices. For these tests it is important that indications of the state of the output devices are provided. Additionally, proper interlocks should be in place to prevent inadvertent plant disturbances.

Most software provided with digital systems provides the ability to force a point to a particular value for testing purposes. As with output device testing, it is critical that indication of the forced points is provided to the maintainer and that the proper interlocks or bypasses are in place to prevent inadvertent plant disturbances.

Resource Management

Many digital systems provide a computer-based Human Machine Interface (HMI) for the system user and maintainer to interact with and maintain the equipment. In nuclear power plants, these HMIs may be operating continuously for months or even years. There is a potential in some cases for HMI-generated log and system files to become very large, thus exhausting the storage capacity of the memory or storage media of the system. These log and system files should be periodically removed and archived if necessary to free-up these HMI resources.

Additionally, HMIs should be re-started periodically to restore system resources that may have become depleted due to conditions such as resource or memory leaks.

The frequency of this activity can be determined by trending system resources (if possible). If not possible, then the authors recommend that this activity should be performed as opportunities arise when the HMI is not needed (e.g. refueling outages).

Failure Detection

This activity is not designed to detect a failure, but to prevent the loss of functionality of a digital system HMI.

Considerations

- Ensure that all necessary logs/files are archived.
- Ensure that all user entered parameters are stored / documented.

Subassembly / Component Level Maintenance

Limited Life Component Replacement

Individual manufacturers should provide recommended component replacement preventive maintenance intervals for their equipment. Most modern digital I&C systems (especially PLCs, DCSs and systems utilizing FPGAs) consist of modules housed in a chassis. Typically the modules are sealed and there are few user serviceable components. Control and communication modules will consist primarily of solid state electronics and will not require regular maintenance. Some I/O modules and field termination cards may have components that are serviceable (e.g. relays, fuses). The following are some general parts that are typically replaced on a periodic basis:

Batteries

Typically these are used to provide power to memory devices within the digital I&C system. The type and size of these vary by manufacturer. The manufacturer's recommendation on a replacement schedule should be followed and incorporated into the component preventative maintenance program. Often these batteries are monitored as part of the system diagnostics. However, since failure of these batteries can lead to loss of functionality and program memory, proactive replacement of the batteries is usually recommended. The typical replacement interval for lithium batteries is five years [2].

Electrolytic Capacitors

Electrolytic capacitors are used in various pieces of equipment in a digital I&C system. They are typically found in power supplies and in some filter circuits. In many modern digital systems, these capacitors are not serviceable by the maintainer. For digital systems where maintenance on electrolytic capacitors is possible, Reference [10] provides a good resource for maintenance practices for electrolytic capacitors. Many of the practices within this reference are directed to maintenance of electrolytic capacitors within power supplies. Recommended off-line maintenance for electrolytic capacitors not specifically part of power supplies from Reference [10] include:

- Capacitance checks
- Leakage current checks
- Dielectric Absorption tests
- ESR tests

Reference [10] also provides information on the typical shelf life of electrolytic capacitors and tests that should be performed before being placed into service. A typical practice for "can" type electrolytic capacitors used in power supplies and other power electronics is to "re-form" the capacitor before placing them into use to restore the dielectric oxide layer that may have been lost during storage.

Fuses

Depending on the environmental conditions (thermal and electrical), fuses can be expected to remain operational for many years before needing to be replaced. It is difficult to determine the remaining life of a fuse that has not blown. Reference [9] provides guidance on replacement intervals for input and output fuses within power supplies.

HMI Hard Drives

The typical life for a computer hard disk drive is five to seven years, although this is highly dependent on the environment and usage patterns of the drive [27]. Most computer operating systems also provide a disk check utility that can be run on demand to discover certain disk errors and even compensate for conditions such as bad sectors be allocating data around them. Currently, most manufacturers of hard disk drives support self-monitoring technology that measures critical drive parameters such as temperature, spin-up time and data error rates. Not all operating systems utilize this data, however, and operating data suggest that monitoring these parameters alone are not enough to reliably predict hard drive failures [28]. For critical applications a periodic replacement strategy may prove most effective.

Power Supplies

Reference [9] provides detailed maintenance practices for power supplies. Condition monitoring tasks consist of checking output voltage and AC current ripple. Periodic maintenance tasks consist of the following:

- Visual inspection and cleaning
- Auctioneering circuit checks
- Overvoltage protection circuit checks
- Line and load regulation checks
- Energize spare power supply test
- Replace electrolytic capacitors
- Replace input/output fuses

Relays

Relays, being electromechanical components are subject to well-known failure mechanisms. (Digital relays should be calibrated and maintained based on manufactures recommendations). Reference [15] provides recommended maintenance practices for electromechanical relays that interface with digital systems. These include:

- Inspection for evidence of thermal degradation
- Inspection for evidence of mechanical damage
- Inspection for evidence of contact damage
- Inspection for evidence of damage from environmental stresses
- Regular cleaning
- Pickup and dropout voltage checks and adjustment

Cooling Fans

Cooling fans can fail due to bearing wearout and excessive heat. Cooling fans often provide an audible indication of impending failure. Some systems monitor fan speed and can detect problems with fan before complete failure.

Condition Monitoring

Perform Thermal Scans of Equipment

Several failure modes of electronic circuits can lead to increased power dissipation. Performing thermal scans of digital I&C equipment can be useful for detecting component degradation. Since electronic circuits come in such a large number of configurations and components have many different characteristics imparted to them from their manufacturing and material, it is nearly impossible to state a normal thermal scan for a digital I&C system should be. The best practice is to take thermal scans of new equipment operating under normal conditions in a typical environment and use them as baselines. The scans can then be trended the over time. These scans can also be used to detect conditions that have altered the thermal management of the system (cooling flow obstructions, excessive dust accumulation on heat sinks, etc.)

Processor Trending

Surveying manufacturers of digital equipment, the following have emerged as the most important items to monitor to prevent digital system failures:

- Status indicators for individual processors such as scan times. Many digital systems have the ability to monitor processor process timing or various system resources and parameters (memory usage, CPU temperature, etc.). This information can be trended to detect impending issues with the equipment.
- Communication status for individual processors. One should look for an increase in communication errors such as dropped packets and increases in data collisions and CRC errors as these can indicate a pending equipment problem.

Nuclear Power Industry Survey for Best Maintenance Practices Results

Many of the survey respondents were able to provide their recommendations for good maintenance practices for digital instrumentation and control systems. In some cases, these practices were being used presently by the system owner / maintainer in other cases, they are practices that the respondent would like to implement based on their experience but have not yet had the opportunity to do so. A list of these practices is presented below.

1. Tailor maintenance intervals to a combination of vendor recommendations, environmental conditions and operating experience.
2. Utilize built-in self tests and diagnostics of equipment
3. Understand the metrics and surveillance that the system runs
4. Examine system log files and understand how to interpret the data
5. Ensure preventive maintenance procedures are consistent with vendor recommendations.
6. Obtain maintenance training from equipment vendor
7. Keep equipment cool and clean
8. Limit power cycling of cabinets
9. Don't "touch" the equipment any more than necessary
10. Consider cyber security as part of preventive maintenance program
11. Supervise vendor maintenance in order to maintain configuration control
12. Purchase extra system, particularly up front, to use for training and trying out fixes, patches, upgrades, etc.
13. Design systems to be single-failure tolerant to permit reactive maintenance strategy for equipment
14. Perform periodic thermal scan of processors and equipment
15. Perform "burn-in" of replacement parts before installing
16. Reboot processor-based systems periodically
17. Consider the creation of stand-alone digital group rather than as part of I&C maintenance
18. Perform periodic Time Domain Reflectometry (TDR) tests on fiber optic cables

While all the items in the above list are regarded as good practices by the authors, some items are worthy of comment. Items 1 through 6 relate to integrating vendor provided maintenance tools and recommendations into the system owner's maintenance program. The value of using and understanding the vendor supplied tests and diagnostics cannot be understated by the authors. For digital systems, the proper utilization of the built-in tests and logs is perhaps the most effective maintenance tool the maintainer has at his or her disposal. Items 7 through 9 focus on the monitoring and reduction of stressors for electronics, particularly thermal, electrical and mechanical stressors. In the absence of data supporting a periodic replacement of digital system components or modules, implementing practices to reduce the stressors that decrease the useful operating life of electronic components is a always a smart strategy for the system maintainer.

Finally, item 10 deserves to be highlighted as a good practice since there have been several cyber security issues that occurred during a maintenance activity reported in the LER and INPO databases.

From the discussion in Section 3 the following additional recommendations are made:

1. Design maintenance activities to address as many of the failures of digital systems as possible since the equipment is already being tested, probed or disturbed and this would be the most cost and time-effective chance to perform a failure mitigation activity. As discussed previously, doing so provides an opportunity to possibly detect any deficiencies missed by other plant processes and procedures.
2. The second recommendation is to tailor maintenance activities to mitigate as many of the stressors of digital electronics as possible. This includes activities such as inspecting and cleaning the equipment and monitoring and reducing the environmental stressors discussed above. The different activities to reduce various environmental stressors are likely to be implemented as one-time modifications (e.g. installing additional cooling equipment, relocating equipment away from sources of vibration, etc.). Once the stressors have been reduced for the equipment, ongoing maintenance activities would consist of monitoring the digital equipment environment.

At least one respondent indicated that they are adopting a Reactive Maintenance strategy for their digital instrumentation and control systems. They are able to accomplish this by designing redundancy into their systems. That is, they are essentially able to tolerate any single failure within their digital systems. This obviates the need for many (but not all) periodic checks and replacements as well as any advanced parameter monitoring to detect impending failure. This strategy can provide a significant savings in routine maintenance. One caution, is that for this to be effective, redundant component functionality must be designed correctly and must be routinely verified or continuously indicated (operating experience has shown several instances of failovers to non-functioning redundant components). The trade-off of course for implementing this strategy, is an increase in the acquisition cost for the equipment as additional hardware is needed.

Ultimately, most system owners / maintainers will find it cost-effective to adopt a combination of the three main maintenance strategies of Reactive, Preventive and Predictive Maintenance. Determining the proper mix of these is usually accomplished through a reliability centered maintenance approach. This methodology acknowledges that not all equipment is of equal value to the facility and that the different equipment will have differing operating lives and be subjected to differing operating conditions.

Reference [20] provides an overview of how to determine which type of maintenance should be performed on specific equipment. Reactive maintenance is well-suited to smaller, less expensive equipment that is not prone to failure and is not essential for the operation of the facility or is part of a redundant system (i.e. there is another piece of equipment that will perform the same functionality of the failed component). Preventive maintenance is best for equipment that has a well-established wear-out or failure mechanism(s) and/or is consumed as a part of the operation of the facility. Predictive maintenance may be appropriate for equipment that has random failure patterns or is critical to the operation of the facility and is not subject to well-known wear mechanisms. This type of maintenance may also be appropriate for equipment that may fail as a result of incorrect preventive maintenance.

Considering the high number of digital failures that are attributable to Human Performance and Inadequate Maintenance Procedures the industry respondents were asked for recommendations on the information to capture during maintenance activities. Admittedly, given the great variation in the types of digital I&C systems in use, it is difficult to create a list of information that is applicable to all systems, however the following were indicated by multiple respondents to be recorded:

- Firmware or software revision
- Circuit card revision number
- Model or part numbers
- Serial numbers of cards, modules or components
- Devices addresses (e.g., IP address)

Additionally, some respondents recommended recording a screenshot of the display or logic diagram before and after the maintenance activity (although, one must be sensitive to cyber security concerns as device names and addresses may be captured).

Further Considerations

From the responses received for this study, it seems that the use of predictive maintenance for digital I&C in the nuclear power industry is still rare. There are many reasons for this such as relatively new digital installations and heavy reliance on vendor for support and training. Discussion with researchers at the Center for Advanced Life Cycle Engineering at the University of Maryland indicate that data-driven prognostic techniques may prove the best candidate predictive maintenance strategy for utilities and plant owners. The key to these methods are having ample data available and the resources and knowledge of how to analyze and look for useful patterns in the data.

Often one is not able to monitor all the variables / parameters to support a prognostic monitoring effort. This can be due to lack of funds, lack of access to the measurement points and/or a lack of knowledge about what to monitor. If the system owner/maintainer is considering pursuing a prognostic health monitoring program for their digital I&C system, the authors recommend consulting reference [29]. This paper discusses how to evaluate the benefits of a proposed prognostic measurement technique from and economic perspective. It provides the formulas and methods to enable the maintainer to evaluate if a proposed monitoring method would provide an overall economic benefit (through reduced maintenance costs). While such methods have been routinely applied to mechanical systems that often provide physical clues indicating impending failure (high vibration, stress fractures, etc.) these techniques have not been widely applied to electronics. This is in large part because of a lack of a predominant failure mechanism for electronics. Indeed, there are a large variety of failure mechanisms for the electronics within a digital system (see section 2) and the large number of potential failure sites (consider an integrated circuit with its hundreds of thousands of internal transistors) that make it difficult to locate a prognostic sensor. However, by treating the system as a black box and considering sensors to monitor more than one failure mechanism can prove to provide a maintenance savings to the owner. The author works through an example of adding prognostic monitoring to an aircraft power supply. The addition of two sensors, one to measure rise time of the switching section and the other to measure the internal power dissipation of the power supply are considered. The resulting analysis shows that the internal power dissipation sensor yields a significant cost savings for maintenance even if the assumptions about cost avoidance per correct prognostic event, efficiency of the prognostic technique or ratio of unscheduled repair time to planned repair time is are not correct. In this example, this is in large part due to the fact that the sensor is inexpensive and it has the ability to detect failure of multiple sections of the power supply.

Recommendations from this paper include [29]:

- Select sensors that are applicable to multiple failure mechanisms
- Target prognostics at black box level because that is where organizational maintenance is performed
- Consider adding sensors to a component when the ratio of unscheduled repair time/cost to planned repair time/cost is high
- Minimize cost of sensors so that savings is high even if the efficiency of the technique is not as high as assumed

5
SKILLS REQUIRED BY PERSONNEL TO PERFORM RECOMMENDED PREVENTIVE MAINTENANCE

In addition to the maintenance activities and practices being performed, each nuclear power industry respondent was also asked about the training provided to their personnel to maintain the digital instrumentation and control systems. The responses were varied.

Almost all of the respondents indicated that either engineers or both technicians and engineers receive training from the equipment vendor upon procurement or installation. This training is to understand the basic operation and programming to perform basic diagnostic functions and modify the code if necessary. At most plants, personnel from the training organization attend the classes as well and incorporate the information into the plant maintenance training program. This is a recommended activity for any new digital system. Based on the data collected from the nuclear industry respondents and the experience of the authors, it is highly recommended that the system owners/maintainers learn how to modify the code or algorithms used in the system as inevitably a change will be required once the equipment has been operational for some time. It is also recommended that all such changes that affect the basic functionality of the system (versus a system parameter change or the like) are reviewed with the vendor beforehand to understand all the consequences to the system by the change.

Some respondents indicated that their technicians receive very detailed training on electronics but only a high-level of training on digital controllers or PLCs. System owners may want to de-emphasize the training in electronics in favor of a greater familiarity with the digital controllers and modules and their operation. This is due to the fact that most modern digital systems are not serviceable by the end-user down the electrical component level. Typically, the vendor-supplied guides and built-in diagnostics and tests permit troubleshooting down to the module or card level. So while a basic understanding of electronics is important, training should focus on the lowest level repairable unit.

Given the ubiquitous nature of PLCs in modern digital instrumentation and control systems, system owners should consider providing PLC training to their system maintainers. Below are two syllabi from two plants that provide a good template of the items that should be covered in such a class.

Training Provided

Plant #1

Programmable Logic Controllers Maintenance Training (Generic):

- Define terms associated with PLC programming
- Identify location, purpose and function of the major components in a PLC

- Identify indicators on various PLC modules and the information they provide
- Describe the process to calibrate analog input/output modules of a PLC
- Examine a failed PLC to determine the information that should be gathered prior to repair of a PLC
- Describe the process to replace a failed module in a PLC, including Human Performance Standards

Specific PLC Maintenance Training (targeted at a particular brand of PLC)

- Define terms relating to the System
- Identify location, purpose and functions of the major components used in the system
- Explain how status lights can be used to determine the operability of the system
- Explain the function and basic operation of the Modules used at the plant
- Describe the function and operation of the External Termination Panels (ETP) used at the plant
- Identify the major components of the controller software
- Explain the steps to playback an event log file using logging software
- Explain how the diagnostic software can be used to troubleshoot the System
- Describe the plant Software Quality Assurance program as it pertains to the system software application
- When given a PLC Familiarization Exercise, determine the appropriate Error Prevention tool(s)

Plant #2

HMI Software and PLC Software (Engineering):

- Architecture, hardware, programming and deployment

For electronic configuration qualification (Engineering):

- Configuration Management Program, Configuration Change Determination, Engineering Configuration Changes, Electrical and I&C Engineering Information, Equipment Database, Plant Walkdowns, Pre-Job Briefs and Post-Job Reviews, Work Management Process, Human Performance Tools, Document Control, Instrument Configuration, Operating Experience.

For I&C qualification (Technicians):

- DCS system overview, troubleshooting, etc.

Additional recommended topics for PLC training classes in-light of the digital control system issues presented in Section 2 include:

- Describe basic PLC troubleshooting techniques

- Describe security features associated with the PLC
- Review administrative and operational plant procedures associated with the PLC

Every person surveyed said that they provide system specific training to the maintenance staff. This obviously is a recommended practice. An enhancement to this practice is to provide the maintenance staff with the knowledge of how the operators use the equipment. Such an understanding facilitates troubleshooting and can even allow the maintenance staff to proactively correct any deficiencies if they test-out any repairs or modifications as the operator of the equipment would.

Other recommended skills and training include:

Use of Mock-up / Simulator for Training

Many of the plants/companies surveyed utilize a mock-up of the installed digital system in order to provide training and to be able to try out potential changes to the installed systems before actual implementation in the plant. Personnel receive vendor training and learn on plant mock-up in training facility.

Implement Formal DCS I&C Qualification

Several of the people surveyed indicated that they have some kind of qualification program for the personnel (typically both system engineers and maintenance technicians) working on digital I&C systems. A key component of these programs is mentoring and knowledge transfer. Such programs require that the person be mentored on certain knowledge areas. Upon completion of the mentoring, a qualification is issued after the person has demonstrated their knowledge to a designated evaluator.

Attend User's Group Meetings

In some cases, attending user's group meetings is part of the plant procedures. Given the specialized nature of the nuclear power industry, such meetings are an invaluable way to share operating experience and best practices.

Cyber Security Training

At a minimum, all personnel with access to the digital I&C equipment should be trained on basic cyber security practices and cyber threat awareness. Topics should include understanding physical, software and network threats to the security of the digital systems as well as how to employ basic controls (security policies, restricting physical access, firewall configuration, etc.).

6
CONCLUSIONS AND RECOMMENDATIONS

Failure data for digital I&C systems from the NRC, EPRI and INPO were categorized by type of failure. The compiled data show that human performance and hardware failure are the two most prevalent causes for digital I&C failures. An average of four to six events per year for each of these categories has been observed over the past five years.

Many of the nuclear power industry respondents as well as those outside of the nuclear power industry report similar maintenance activities for their digital I&C systems. This, coupled with the relatively low-number of hardware failures reported annually, suggest that for the most part, the proper maintenance is being performed on these systems.

One recommendation for improvement is to increase training for system maintainers in the use of vendor supplied monitoring and diagnostics features. Through interviews with both the system owners and the equipment manufacturers, it appears that the built-in monitoring and testing provided by manufacturers are not always utilized to the fullest extent. This can be due to both unfamiliarity with the equipment and its capabilities or limitations imposed by the application of the equipment in a nuclear power plant. Providing this training has the potential to reduce the number of system failures due to hardware failure observed within the industry.

A further recommendation is to use maintenance activities as opportunities to bolster other plant processes that are used to prevent system failures. For example, one respondent reported that when they replace power supplies as part of their routine maintenance program, they also verify the configuration of the new device matches that of the one being replaced as well as that provided in plant documentation. As a result, this activity provides an additional check to prevent system failure as a result of a configuration management or human performance issue. As this example illustrates, a side benefit of using maintenance activities as an opportunity to check or verify against multiple types of digital system failures, is that it has the potential to catch many other types of digital system issues before they manifest themselves as failures.

The optimum condition to establish a component reliability program would be to have years of detailed, historical, and accurate data on all major failure modes for a component type. Unfortunately, that does not exist for the bulk of plant equipment. The best facsimile to a perfect data set is to gather a group of equipment experts—whose livelihood has depended on the availability of the equipment in question—and systematically gather their experience. Therefore, follow-on work should focus on the development of Preventive Maintenance Basis Database (PMBD) tables for digital systems. To accomplish this, the Expert Elicitation procedure presented in EPRI document 1023073 [30] should be used.

The following is the general procedure used for these sessions.

- Designate component type: A clear title that communicates the component analyzed where it is sometimes differentiated by a number of factors including design, service type, and capacity.

- Establish boundary: A statement that establishes what is included and explicitly excluded from the boundary of the component or system.
- Define duty cycle and identify equipment stressors: Define how duty cycle and environmental stressors challenge equipment availability.
- Identify component reliability tasks: Identify those tasks that provide information on component material condition and performance, including condition monitoring, performance monitoring, and preventive maintenance tasks.
- Develop degradation modes: This process stage lists all of the subcomponents, any reasonable way in which those subcomponents fail, and the causes for that failure along with a number of other factors.
- Determine component task effectiveness: The elicitation team comes to a consensus on the scope of the component tasks and on the task effectiveness for each degradation mode/component task combination.
- Summarize elicitation: A final review of the previous work and wrap-up tasks that complete the following fields: maintenance risk, common failure causes, and industry references.
- Analyze results: In this stage, the facilitators will complete all component task fields and adopt baseline intervals, create task ranking, build as-found condition checklists, perform the peer review, and test the component data table in the analysis software.

This results in a matrix provides the basis for a reliability-center maintenance (RCM) for individual end users to properly define and schedule maintenance and monitoring tasks with a comprehensive list of degradation and failure modes from real-world experience.

7
REFERENCES AND BIBLIOGRAPHIES

References

[1] US Energy Information Administration, "Frequently Asked Questions." Internet: http://www.eia.gov/tools/faqs/faq.cfm?id=228&t=21, [January 18, 2013].

[2] *Practical Maintenance of Digital Systems Guidance to Maximize the Benefits of Digital Systems and Plant Equipment*, EPRI, Palo Alto, CA: 2004. 1008124.

[3] *Digital Control Systems: Survey of Current Preventive Maintenance Practices and Experience*, EPRI, Palo Alto, CA: 2011. 1022713.

[4] J. Gu, N. Vichare, T. Tracy and M. Pecht, "Prognostics Implementation Methods for Electronics," presented at the Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL (January 2007).

[5] *Industry Survey of Digital I&C Failures*, Oak Ridge National Laboratory, Oak Ridge, TN: 2007. ORNL/TM-2006/626.

[6] *A Survey of Electronics Obsolescence and Reliability*, Australian Government Department of Defence, Defence Science and Technology Organisation: Fairbairn, Canberra: 2010. DSTO-TR-2437.

[7] Digital Instrumentation and Controls, Task Working Group #4: *Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance, Revision 1*, US NRC, Washington, D.C.: 2009.

[8] *UPS Maintenance and Application Guide*, EPRI, Palo Alto, CA: 2002. 1003466.

[9] *Power Supply Maintenance and Application Guide*, EPRI, Palo Alto, CA: 2001. 1003096.

[10] *Capacitor Application and Maintenance Guide*, EPRI, Palo Alto, CA: 1999. TR-112175.

[11] J. McLinn, "The Simple Fuse," *IEEE Reliability Society 2008 Annual Technology Report*. 2008.

[12] *Printed Circuit Board Maintenance, Repair, and Testing Guide*, EPRI, Palo Alto, CA: 2003. 1007916.

[13] *Preventive Maintenance Strategy for Data Centers*, APC, W. Kingston, RI: 2007. White Paper #124.

[14] J. Srinivasan, S. Adve, P. Bos, J. Rivers, "The Case for Lifetime Reliability-Aware Microprocessors," *Proceedings of The 31st International Symposium on Computer Architecture (ISCA-04)*, (1994).

[15] *Maintenance and Application Guide for Control Relays and Timers,* EPRI, Palo Alto, CA:1993. TR-102067.

[16] *Guidelines for Electromagnetic Interference Testing of Power Plant Equipment: Revision 3 to TR-102323*, EPRI, Palo Alto, CA: 2004. 1003697.

[17] R. C. Dorf. *The Electrical Engineering Handbook*. CRC Press, 1997, p.2136.

[18] *Protecting Against Digital Common-Cause Failure*, EPRI, Palo Alto, CA: 2010. 1019182.

[19] *Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems*, EPRI, Palo Alto, CA: 2008. 1016731.

[20] Federal Transit Administration, "O&M Best Practices Guide," Release 3.0.

[21] *Reliability Centered Maintenance Guide for Facilities and Collateral Equipment*, NASA: 2000.

[22] *Evaluating the Effects of Ageing on Electronic Instrument and Control Circuit Boards and Components in Nuclear Power Plants*, EPRI, Palo Alto, CA: 2005. 1011709.

[23] J. G. McLeish, "Enhancing MIL-HDBK-217 Reliability Predictions with Physics of Failure Methods," presented at the Annual Reliability and Maintainability Symposium (RAMS), San Jose, CA (January 2010).

[24] N.M.Vichare, M. G. Pecht, "Prognostics and Health Management of Electronics," *IEEE Transactions on Components and Packaging Technologies*. Vol. 29, No. 1, pp. 222-229 (2006).

[25] H. Kabza, H.J. Schulze, Y. Gerstenmaier, "Cosmic Radiation as a Cause for Power Device Failure and Possible Countermeasures", *Proceedings of The 6th International Symposium on Power Semiconductor Devices and IC's*, Davos, Switzerland (1994).

[26] *Failure Rates of Fast Recovery Diodes Due to Cosmic Rays*, ABB, Lenzburg, Switzerland: 2012. Doc. No. 5SYA 2061-00.

[27] *C. Shaohsin, S. Feng-Bin, J. Yang, "A new method of hard disk drive MTTF projection using data from an early life test,"* Annual Reliability and Maintainability Symposium (RAMS), Washington, DC, 1999.

[28] *V. Argawal, C. Bhattacharyya, T. Niranjan, S. Susarla, "Discovering Rules from Disk Events for Predicting Hard Drive Failures,"* International Conference on Machine Learning and Applications, Miami Beach, FL (December 2009).

[29] H. Hecht, "Prognostics for Electronic Equipment: An Economic Perspective," presented at the Annual Reliability and Maintainability Symposium (RAMS), Newport Beach, CA (January 2006).

[30] *Guideline for Expert Elicitation of Equipment Reliability Experiences*, EPRI, Palo Alto, CA: 2011. 1023073.

[31] J. Brusse, H. Leidecker, L. Panashchenko, "Metal Whiskers: Failure Modes and Mitigation Strategies," presented at Dominion Printed Circuit Board Reliability Conference, Glen Allen, VA (February 2008).

[32] Q. Sun, G. Selvaduray, "Understanding and Minimizing Tin Whiskers – A Review of the Literature," Internet: http://www.sjsu.edu/faculty/selvaduray/page/recent/TinWhiskers.pdf. June 04, 2003 [June 02, 2013].

[33] M. Sampson, H. Leidecker, "Basic Information Regarding Tin Whiskers," Internet: http://nepp.nasa.gov/whisker/background/index.htm. [June 02, 2013].

[34] M. Osterman, "Mitigation Strategies for Tin Whiskers," Internet: http://www.calce.umd.edu/lead-free/tin-whiskers/TINWHISKERMITIGATION.pdf. July 3, 2002 [June 02, 2013].

[35] "Resolution of Generic Safety Issues: Issue 200: Tin Whiskers (NUREG-0933, Main Report with Supplements 1–34)," Internet: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0933/sec3/200.html. March 29, 2012 [June 02, 2013].

[36] *HP experience with tin whisker inspection training*, Hewlett-Packard Development Co., Houston, TX: 2005.

A
APPENDIX A – METAL WHISKERS AND REMEDIATION ACTIVITIES

Metal Whiskers

Metal whiskers are electrically conductive, crystalline structures that grow spontaneously from plated tin (or zinc) surfaces. These structures can be anywhere from 0.3 to 10 µm in diameter but typically are 1 µm or less in diameter. Than can grow up to 10 mm in length, which is rare, but are usually around 1mm long [31][32][33]. They can grow without an electric field present and are found in many shapes such as straight, bent, kinked, forked or even hollow [32][33].

Researchers report that growth of tin whiskers may occur from days to years and rate of 0.03 to 9 mm/yr have been observed [33]. They seem to grow best between 25°C to 75°C and growth ceases above 150°C [32][33].

These whiskers are coated with electrically insulating films and so direct mechanical contact between whisker and conductor does not guarantee electrical contact. The voltage potential between the whisker and the conductor must be sufficient to exceed the dielectric breakdown of the insulating film. This can be in the range of 0.2 to 45 V [31].

Metal whiskers were known at least as far back as 1946 (cadmium whiskers). Bell labs researched materials that when added to a tin coating would prevent whiskering. They determined that adding 0.5 – 1% by weight of lead worked. Since the 1990s the US military has required of its suppliers that lead be added to any tin coatings used around electronics [31][32].

Tin/lead solder was used by the electronics industry for many years due to solderability and reliability characteristics. The European Union Reduction of Hazardous substances (RoHS) Directive that went into effect in 2006 has contributed to reduced usage of lead-free solder by most electronics manufacturers and has driven the development of lead-free replacement of the tin-lead coating used in lead-frames and printed circuit boards [6].

At present, there is no universally applicable replacement for tin/lead solder. Several replacement solder compositions have been developed, with tin/silver/copper (Sn-Ag-Cu) being the most prevalent. The lead-free transition continues to present reliability and manufacturing issues for the electronics industry. Especially hard-hit are manufacturers of products used in high-reliability applications [6].

Nuclear Power Industry Experience with Metal Whiskers

The US NRC has compiled a historical record of tin whisker events as documented at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0933/sec3/200.html [35]:

In 1987, Dresden Nuclear Power Station Unit 2 experienced a trip of the “B” channel of the RPS due to a metallic whisker that grew on the fission chamber outer electrode creating a temporary short circuit that subsequently cleared by melting away [35].

In the spring of 1990, Duane Arnold Nuclear Energy Center experienced an automatic reactor SCRAM during startup as a result of a metal whisker induced short circuit on an LPRM detector [35].

In 1997 at Dresden Unit 2, a reactor SCRAM occurred when a short circuit was caused by a metal whisker within an LRPM detector [35].

On September 1, 1999 South Texas Project Unit 2 a reactor pre-trip alarm occurred due to the failure of an input control relay for low-low level on the steam generator attributed to tin whiskers [35].

In April of 2005, Millstone Unit 3 experienced a reactor trip along with an actuation of one of two trains of Safety Injection and Main Steam Isolation resulting from a short circuit to ground caused by a tin whisker on a Solid State Protection System logic card [35].

The US NRC considers all of these events to fall within the scope of the maintenance rule and as such has determined that no new rules or regulations are needed.

Metal Whisker Failure Modes

Continuous Short Circuit

It is possible for metal whiskers to create a continuous short in circuits that are operating at low voltage and have high impedance. The amount of current flowing through the whisker in this case may not be enough to “open” the whisker [33][34].

Transient Short Circuit

It is possible that the metal whisker can lead to a transient short circuit condition. This can happen if the available current into the tin whisker exceeds the fusing current of the whisker. In this case, only a transient glitch is experienced by the circuit [32][33][34].

Debris and Contamination

Whiskers or parts thereof, my break loose from the surfaces from which they grew and create shorts in circuits or bridge isolation barriers. Additionally, these whiskers and fragments may interfere with optical components [33][34].

Electromagnetic Interference (EMI)

At frequencies above 6 GHz, metal whiskers can act like miniature antennas, affecting the impedance of digital circuits [6].

Determining if Metal Whiskers are Present

The most basic equipment needed to inspect for metal whiskers is a binocular microscope and a light source. The literature suggests that multiple angles of inspection or light source are needed to effectively determine the presence of metal whiskers. Therefore, a flexible light source or tilt table is recommended. NASA GSFC has published videos to aid in the optical inspection of tin whiskers (http://nepp.nasa.gov/whisker/video) [31][33]. Unfortunately, visual inspections for tin whiskers will not always lead to the detection of tin whiskers. A study by HP found that a group of trained inspectors using JEDEC methods did not always detect the same tin whiskers on identical hardware. Additionally, determination of whisker density by the inspectors varied and it was concluded that a whisker density of "medium" could not be reliably determined [36].

Such inspection, of course, is all predicated on the ability to gain access to the electrical circuit in order to make a visual inspection. This can be difficult with many modern digital instrumentation and controls where the constituent parts of the system are comprised of sealed modules.

Tin Whisker Mitigation

There are steps that can be taken to reduce the possibility of tin whiskers.

- Avoid the use of pure tin plated components if possible [31][33].
- Select a matte or low-stress tin finish [6] (plating thickness below 0.5 µm and above 20 µm are the relatively "safe" ranges) [32].
- Vary the thickness of tin plating [34].

Where the above steps are not possible, the following are recommended:

1) "Solder dip" the plated surfaces using a tin-lead solder [33].
2) Conformal coat or use foam encapsulation over the whisker prone surface [31] [33] [34].
    a) NASA Goddard Whisker Mitigation Study Conformal Coat (Uralane 5750 Polyurethane) showed that 2 mils of Uralane was very effective in trapping tin whiskers [31].
    b) Other coatings that are not optimal can offer some protection against a whisker coming from a distant source as long whiskers tend to bend and break easily [31]
    c) Conformal coatings also provide protection from loose conductive debris (possibly from broken tin whiskers) [34].
3) Re-plate the whisker prone areas [31] [33] [34].
4) Avoid applying compressive loads on plated surfaces [34].

Metal Whisker Practices in the Nuclear Power Industry

The respondents to the survey were questioned about their tin whisker mitigation practices. Many of them reported that they handle tin whiskers on a case-by-case basis with the exception of certain safety related equipment (particularly Solid State Protection System circuit cards) where almost everyone implements some kind of prevention activity. This primarily consists of visual inspection and cleaning such as using special vacuum cleaners and de-ionized air in order to remove any whiskers or whisker debris.

Some respondents indicated that they provide guidance for repair and refurbishment of what type of solder can be used during the process. Also, many rely on vendors to identify any issues with tin whiskers.

The general consensus was that significant issues with tin whiskers are rare in the nuclear power industry (as corroborated by reference [35]).

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

Program:

Nuclear Power

3002000502

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com