

ASSESSMENT OF DIGITAL SYSTEM OPERATING EXPERIENCE DATA AND SYSTEM INVENTORY AND CLASSIFICATION STRUCTURE

INTRODUCTION

The Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) has been reviewing digital system operating experience (OE) data and system classification structures as part of activities in the NRC Digital System Research Plan [1]. The RES reviews have also addressed recommendations from the Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Control (DI&C) and the Digital I&C Project.

The ACRS suggested that by classifying the various digital systems used in safety critical applications in nuclear power plants, the staff could determine which systems should be analyzed for diversity and defense in depth (D3) and at what level of detail. A digital system classification structure is intended to be used for two primary purposes; first to provide insight to digital systems OE evaluations, and second to support and inform ongoing development of digital system D3 regulatory guidance.

Actions based on the ACRS recommendations were added to the Digital I&C Project Plan for the D3 Task Working Group (TWG) #2, "Diversity and Defense-in-Depth," under two milestones (see Figure 1). In September, 2007, RES issued a white paper, "Preliminary Assessment of Major Issues or Common Themes in Inventory and Classification and Operating Experience Evaluation for Digital I&C Systems" (ML072710480) [2]. The primary goal of the preliminary assessment was to validate the interim staff guidance (ISG) for D3 or recommend changes. No changes to the D3 Interim Staff Guidance were necessary.

The staff's subsequent efforts at evaluating digital system OE data and classifying digital systems to identify applicable diversity approaches for regulatory guidance are described in this assessment report. The background section provides a technical and regulatory perspective of D3 and Common Cause Failures (CCF), and an overview of NRC staff activities to a) gain an understanding of the types of failures that have occurred in digital systems and b) the need for classifying systems within the context of their application environment. Section I then discusses the sources of digital industry failure data that have been or should be reviewed by the staff to determine appropriate diversity attributes. Section II describes the classification structures for digital systems and how classification relates to diversity strategies. Finally, Section III provides concluding remarks and recommendations.

BACKGROUND

A digital system classification structure consists of categories that capture the key attributes of the system in a manner that supports consistent descriptions of the various digital systems installed or planned for the nuclear power industry. The classification structure could support digital system regulatory reviews and consistent failure data capture and analysis. One regulatory purpose for developing a digital system inventory and classification is that the information obtained through performing these activities could be used in the development of regulatory guidance on D3 for DI&C systems.

Enclosure

A digital system classification structure also will support improved DI&C OE evaluation by providing a consistent structure for categorizing failure data. A key objective of evaluating digital system OE is to determine potential common cause failure (CCF) vulnerabilities in digital systems and then use that information to determine the degree of diversity and defense in depth (D3) necessary to protect a safety function against the occurrence of a digital system failure due to a common cause.

Protecting digital systems against CCFs demands high quality in the system development process. Even with the assumption of high quality the potential for CCFs cannot be excluded. A typical approach for avoiding or mitigating errors that could lead to CCFs is to incorporate diverse features into a system design such that a single defect leading to a CCF would be unlikely to prevent the system from accomplishing its intended functions.

The regulatory basis for using diversity to avoid or mitigate CCFs is found in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" [3]. In particular, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that "... (1) no single failure results in the loss of the protection system...." Also, GDC 22, "Protection System Independence," requires that, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

NUREG/CR-6303 [4] was developed to provide licensees and the staff guidance for assessing whether diversity is required for avoiding or mitigating CCFs in digital safety systems. NUREG/CR-6303 defined a process for evaluating diversity in nuclear power plant control system designs, and identified the following six diversity attribute categories to facilitate assessments of adequate diversity in safety systems:

- Design diversity
- Equipment diversity
- Functional diversity
- Human (system development life cycle process) diversity
- Signal diversity, and
- Software diversity

The approach described in NUREG/CR-6303, while comprehensive, has been difficult for licensees to apply and for NRC staff to use to confirm that acceptable diversity had been identified and implemented in safety system designs as licensees began replacing existing analog-based safety systems with digital safety system upgrades. Regulatory uncertainty arose from the lack of specific NRC staff guidance regarding the combinations of diversity attributes and associated attribute criteria most likely to result in a safety system design that was not vulnerable to CCFs.

In an effort to address the difficulties (and licensing uncertainty) with applying the NUREG/CR-6303 diversity guidance, the NRC staff has been developing more specific guidance for identifying appropriate diversity approaches. In September 2006 the NRC staff

initiated research [5] to identify sets of NUREG/CR-6303 diversity attributes and associated diversity attribute criteria that could complement other design approaches as part of a comprehensive process for confirming that a design had appropriately addressed CCF vulnerabilities. The information obtained from this research project is being used to develop: a) technical guidance for the staff on appropriate CCF avoidance and mitigation measures using the NUREG/CR-6303 diversity attributes and associated attribute criteria; and b) regulatory acceptance criteria complementing existing NRC regulatory processes for confirming that appropriate CCF strategies have been implemented.

On November 8, 2006, the NRC Commission conducted a public meeting with the nuclear power industry and NRC staff to discuss DI&C system issues facing the nuclear power industry. The transcript of the meeting may be found on the NRC public web site [6]. One of the recommendations arising from that meeting was that the NRC staff create the Digital I&C Steering Committee to oversee development of regulatory guidance on the use of DI&C systems in nuclear power plants.

In February 2007, under the direction of the Digital I&C Steering Committee, the NRC staff created TWG #2 to develop guidance for addressing diversity and defense-in-depth issues in digital safety systems. Seven issues concerning diversity and defense-in-depth were identified. Six issues involved identification of the need for diversity and defense-in-depth. The remaining issue was to identify safety system design features that constitute an acceptable amount of diversity. This need for confirming that an acceptable amount of diversity had been achieved meshed well with the ongoing diversity research.

A specific diversity approach used in a safety system design depends on the safety system architecture within the context of the whole plant design. Consequently, in developing different diversity approaches to avoid or mitigate CCFs, the NRC staff determined that it is important to ensure the diverse design features incorporated into a safety system are appropriate for the types of nuclear power plant systems the nuclear industry proposes for digital system upgrades or installation. This conclusion resulted in the development of a proposed system classification method for identifying appropriate diversity approaches relative to the system under consideration. This system classification approach was described in the September 2007 preliminary assessment [2] and is discussed in section II of this assessment report.

The ACRS recommended that the diversity strategies developed by the ongoing NRC research project should address the types of failures observed in the digital industry. As discussed in the September preliminary assessment [2] and section I of this assessment report, RES has conducted several reviews to obtain and review DI&C system OE from both the nuclear and non-nuclear industries. To the extent supported by the quality of the data, insights from evaluation of the OE information will be factored into on-going development of D3 strategies and regulatory guidance development. Section I of this assessment report discusses and evaluates sources of DI&C OE data that have been or will be reviewed by RES to obtain insights regarding potential failure modes.

I. ASSESSMENT OF SOURCES OF DIGITAL INDUSTRY FAILURE DATA

In the September 2007 preliminary assessment [2] described above, RES identified several potential sources of digital I&C OE data that would be readily available. The sources of information included nuclear industry OE data derived primarily from Licensee Event Report (LER) data and sources of non-nuclear industry DI&C system OE. Subsequently, the NRC staff identified additional sources of digital system failure event data. The sources reviewed to date include:

- NRC Reactor Operating Experience Program
- NRC Common-Cause Failure Database and Analysis System
- Organization for Economic Cooperation and Development (OECD) joint project to facilitate the exchange of operating experience on computer-based systems important to safety (COMPSIS)
- Institute of Nuclear Power Operations (INPO) Equipment Performance and Information Exchange (EPIX) data base
- Oak Ridge National Laboratory Industry Survey of Digital I&C Failures (aviation, petrochemical, telecommunications, and transportation)

Additionally, the NRC staff is coordinating with the following sources of information to acquire digital system failure data from sources outside the nuclear power industry:

- Additional non-nuclear sources identified by ORNL (Table 2);
- Department of Defense; and
- National Aeronautics and Space Administration (NASA).

Typically, the classification of the failure data in the above data bases is by system category, components within the system, and the type of failure within the component. For example, system categories in the data bases described in the following sections include the auxiliary feedwater system, the containment spray system, and the high-pressure safety injection system. These systems are further categorized by components within the system. For example, components in the auxiliary feedwater system include check valves, motor-driven valve operators, motor-driven pumps, instrumentation and control system components, etc.

The sources of digital system failure data information considered in this assessment are described in the following sections, with an evaluation of the applicability of the failure data to development of diversity strategies using the diversity attributes described in NUREG/CR-6303.

I.1 NRC Operational Event Report Database

The U.S. Nuclear Regulatory Commission (NRC) has an effectively coordinated program to systematically review OE gained from the nuclear power industry and research and test reactors; assess its significance; provide timely and effective communication to stakeholders; and apply the lessons learned to regulatory decisions and programs affecting nuclear reactors. Each licensee must send information to NRC about certain "reportable events" that occur at their facility or during their use of nuclear materials. The reported events are reviewed by NRC staff technical experts using plant specific risk insights and other operating experience to identify significant issues in plant design, operation, or equipment.

Sources of OpE information include

- Daily Event Notifications (10 CFR 50.72)
- LERs (10 CFR 50.73)
- Regional daily events briefings
- NRC Inspection Findings
- International Atomic Energy Agency (IAEA) and Nuclear Energy Agency (NEA) Incident Reporting System (IRS) reports
- INPO documents
- 10 CFR Part 21 reports, and
- Other internal and external studies.

OE reviews are conducted over two time frames, long-term and near-term.

Long-term reviews are performed as comprehensive studies in which typically many years of OE information are aggregated and evaluated from a technical perspective. Generally, these reviews are performed by RES. The study results are integrated into the regulatory process, as appropriate. There are many types of long-term reviews, such as system and component studies, risk and reliability studies, studies of engineering issues, and long-term trending and analyses.

Near-term studies address issues that are covered by regulatory requirements, and focus on determining safety significance and assessing generic implications for OE applications. Consistent with MD 8.7, the NRC created OE Technical Review Groups (TRGs) for distinct technical areas that align with the existing OE Community Topical Groups [8, 9]. One of the TRGs evaluates I&C-related failures, including DI&C. The TRG framework is described on the NRC OE Web page (<http://nrr10.nrc.gov/forum/index.cfm?selectedForum=03>).

The I&C TRG systematically reviews OE community communications and other sources of OE information available for review on the Reactor OE Information Gateway Web page (<http://nrr10.nrc.gov/ope-info-gateway/index.html>) to identify significant issues impacting safety, negative trends, and recurring events to enhance operation safety in nuclear power plants. The TRG review conclusions may involve informing internal and external stakeholders, taking regulatory actions, and/or enhancing NRC programs. The I&C TRG provides updates on industry events every six months. The latest report available on the OE web site is dated June 2007.

Three I&C TRG biannual reports have been submitted to the OE Gateway Web page as of February 2008: “Technical Review Group (TRG) Inputs for February 2006;” “Technical Review Group (TRG) Inputs for August 2006;” and “Technical Review Group (TRG) Inputs for June 2007.” The I&C TRG reviews revealed a number of digital system-related failures; however, the extent and level of causal analysis detail for DI&C in the summaries are not sufficient for mapping failure trends to diversity strategies using the diversity attributes described in NUREG/CR-6303.

1.2 NRC Common-Cause Failure Database and Analysis System

The NRC and the Idaho National Laboratory (INL) developed the Common Cause Failure Database and Analysis System (CCF DAS) to maintain a database of CCFs in the U.S.

commercial nuclear power industry [10]. The purpose of this effort was to develop a process for using the data to estimate probabilistic risk assessment CCF parameters. Equipment failures that contribute to CCF events are identified through searches of the Nuclear Plant Reliability Data System (NPRDS), which contains component failure information prior to 1997; the INPO EPIX database, which contains component failure information since 1997; and the Sequence Coding and Search System (SCSS), which contains Licensee Event Reports (LERs). All events that meet the criteria for a CCF are included in the CCF DAS. The database contains CCFs beginning in 1980 and is continuously updated to remain current.

All LERs submitted by licensees are reviewed for events applicable to the program. Data analysts evaluate the LER and the EPIX report narratives of events to determine the system, component, failure mode, degree of degradation, and plant status. The LER events also are compared to EPIX events to prevent duplication of event reports.

Nuclear power plant systems and associated failures are classified into four categories: the system, components of the system, sub-components comprising the system components, and piece-parts comprising the sub-component. The system category identifies the power plant system affected. For example, for an emergency diesel generator system, a sub-component of the system would be the I&C, and parts of the I&C sub-component could be fuses, a governor assembly, a load sequencer, piping, relays, sensors, etc. In the CCF DAS, I&C are classified as a sub-component of a system component. The piece-parts of I&C sub-components include fuses, relays, sensors, etc.

Software is classified as a piece-part of a sub-component. However, this is the lowest level of the software description related to the cause of a software failure in the CCF DAS. While this granularity in failure data root cause analysis is sufficient for many analytical purposes including developing PRA models (in which software failures can be addressed as a piece-part failure of a sub-component), more specific details are required for identifying appropriate NUREG/CR-6303 diversity approaches. Consequently, the CCF DAS does not provide sufficient causal detail for software-related failures to support developing diversity strategies using the diversity attributes described in NUREG/CR-6303.

I.3 Computer-Based Systems Important to Safety (COMPSIS) Project

The COMPSIS project overall objective is to improve safety management and the quality of risk analysis of computer-based systems including DI&C systems. Software and hardware faults in safety-critical systems are typically rare and consequently most countries do not experience enough of them to be able to draw any meaningful conclusions after their occurrence. To overcome this disadvantage, information from several countries has been gathered in several joint projects, which has led to the creation of the COMPSIS project.

The COMPSIS project [11] is administered under the umbrella of the Organization for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA) and its Committee on the Safety of Nuclear Installations (CSNI). The COMPSIS project is supervised and managed by a steering group composed of national coordinators and additional experts from the project's member countries. The Institute for Energy Technology in Halden, Norway, is the COMPSIS project Operational Agent (Clearing House).

Reports addressing computer based system events are intended to give a broad perspective of events and incidents occurring in DI&C systems and to convey the insights and lessons learned to the international nuclear community. Sources of OE information include events reported by participating member countries on the basis of the participating country national reporting criteria. The reporting is based on national licensee event reports (LERs) and other available documents.

Event coding guidelines [11] provide a DI&C classification structure that is designed to support failure data input and analysis. The COMPSIS classification structure uses the typical system, component, and failure cause categories, but also has categories that stress overall plant impacts from the event. Failures are categorized as follows:

- Other instrumentation and control failure
- False response, loss of signal, spurious signal
- Oscillation
- Set point drift, parameter drift
- Computer hardware deficiency
- Computer software deficiency
- Computer system deficiency
- Unknown computer fault

Each event is analyzed in detail to determine the direct and potential impact on plant safety functions. The analysis identifies the common involvement of operation and safety systems, and the special aspects of I&C functions, hardware, and software. Key points of the analysis focus on the following areas:

- Identification and description of the involved I&C functions;
- Identification and description of the hardware malfunctions and the failed hardware systems, components, and modules;
- The role of hardware redundancy in the event proceeding;
- Identification and description of software malfunctions and software failures for the following software categories:
 - Off-line software for engineering, configuration, and maintenance (e.g. engineering tools, code generator, compiler, linker, locator)
 - On-line software that is running on the computer modules of the system
 - System software (e.g., runtime environment, function block libraries, operating system, communication software, software for self monitoring, start-up, maintenance and troubleshooting)
 - Application software (e.g., function diagram modules)
- I&C handling of malfunctions due to human interaction (e.g. periodic test, maintenance, etc.)
- I&C configuration management (e.g., bad procedures, bad manuals for software modification)

As can be seen in the above list, the COMPSIS database covers a broad range of failure categories that support analyses of DI&C events. However, the level of detail in the software failure categories does not readily support developing diversity strategies using the diversity attributes described in NUREG/CR-6303.

As a member of the COMPSIS project, the Republic of China Atomic Energy Commission (AEC) provided a pilot analysis of COMPSIS events as an action item for the 6th COMPSIS meeting [12]. The AEC report concluded that nuclear safety systems are becoming heavily dependent on computers, networks and software. Therefore, more and more events are being reported in the COMPSIS databank. Due to time limitations, the AEC only analyzed 35 events from the COMPSIS databank. In order to improve analysis precision, the AEC concluded that more events are needed to support their research. The AEC expects to explore cause patterns and event trends in the future. The AEC further concluded that;

- (1) Design defects, configuration management and hardware failures are the three main root causes
 - (a) The origin of design defects are from errors in system requirements. A well-defined requirement analysis and consistent specification could improve system safety and reliability;
 - (b) Configuration management and hardware failure are two factors of influence in the site maintenance phase; and
 - (c) Hardware aging effects can be mitigated by improving component materials.
- (2) Safety system designs should be simple, easy to maintain, and should have detailed procedures for modifying the system.

The AEC also proposed a classification system to represent sources of digital system failures. The proposed classification system consists of the following seven categories:

- Design
- Hardware Failures
- Communication
- Quality assurance (QA)
- Configuration management
- Human factors
- Routine maintenance

The failure categories identified by the AEC can be correlated to the six diversity attributes defined in NUREG/CR-6303 as shown in Table 1. Therefore, if the level of detail in COMPSIS failure data can be improved there is potential for using this information for developing or validating diversity strategies using the diversity attributes described in NUREG/CR-6303.

I.4 Institute of Nuclear Power Operations (INPO) EPIX Data

To support continuous improvement and shared learning, the commercial nuclear industry reports extensive plant, system, and component event and failure data via the EPIX system. EPIX is a database containing statistics on component failures and other engineering information that is maintained by INPO. A Memorandum of Agreement (MOA) (ML060060035) between NRC and INPO [13] provides the general parameters regarding the coordination of activities between these two organizations. These activities include, but are not limited to:

exchange of operational experience data; coordination of inspections and evaluations; and coordination of NRC and INPO training related activities.

EPIX data is used by the NRC in the NRC Reliability and Availability Data System (RADS) [14] and the Common Cause Failure Database System (see section 1.2 above) [10] to estimate PRA parameters for risk-informed safety system designs and to support development of risk insights on the basis of nuclear plant performance history. Additionally, NRC uses the EPIX data to update failure probabilities and failure rates in NRC Standardized Plant Analysis Risk (SPAR) models. Where applicable, the data from the EPIX database has also been used to augment failure data input into COMPSIS format to facilitate data usage for identifying trends in DI&C failures. With additional targeted analysis, EPIX data also could be useful for identifying proposed diversity strategies by identifying diversity attributes that are the most significant contributors to common cause failures.

The Reliability and Availability Data System (RADS) is a database and analysis tool developed by INL for the NRC. The tool is designed to estimate industry and plant-specific reliability and availability parameters for selected components in risk-important systems and initiating events for use in risk-informed applications. The RADS tool contains data and information based on actual operating experience from U.S. commercial nuclear power plants. The data contained in RADS is kept up-to-date by loading current EPIX data and by yearly updates of initiating event data from licensee event reports (LERs) and other sources. The reliability parameters estimated by RADS are (1) probability of failure on demand, (2) failure rate during operation (used to calculate failure to run probability), and (3) time trends in reliability parameters.

The EPIX data is at the component and sub-component level. Currently, the level of EPIX data detail used by the NRC is sufficient for PRA applications. However, this level of detail is not sufficient for developing NUREG/CR-6303 diversity strategies as root cause analysis information must be identified. An extensive review of the EPIX data for the purpose of identifying root cause failure data for NUREG/CR-6303 diversity strategies would be required to identify information supporting specific diversity strategies. RES intends to work with the INL and INPO to identify processes for obtaining more detailed information on root causes of DI&C failures.

1.5 ORNL Letter Report, “Industry Survey of Digital I&C Failures”

As part of the DI&C Research Plan [1], RES initiated an ongoing task, “Industry Survey for Digital I&C Failures,” within the Emerging Technologies project to investigate DI&C failures in safety-critical systems to document the failure mechanisms and failure modes of digital systems [7]. In particular, this task surveyed the nuclear and non-nuclear industries for available sources of DI&C failures. The non-nuclear industries reviewed included aviation, petrochemical, telecommunications, and transportation. The ORNL letter report documents the results of a survey of available sources of DI&C failures in nuclear and non-nuclear industries, with a focus on the latter. The following discussion summarizes the results of the survey.

The *Aviation Safety Information Analysis and Sharing (ASIAS)* system was searched for digital-instrumentation-related incidents. The total number of reports in the database was 86,682, which represents data from 1978 to December 2006. From these reports, 67 incidents were

identified as computer-related. The typical failure mode given was that the computer “failed.” Detailed failure modes were not provided, which limited the usefulness of this data.

In the petrochemical industry, the *Offshore Reliability Data* (OREDA) system was reviewed for failures related to control and processing. Most of the available offshore reliability data dealt with mechanical and electromechanical equipment. Because the focus of the ORNL review was on DI&C equipment, only the small subset of the data that was DI&C-related was analyzed. This included the “Control and Safety Equipment” category as well as the control systems in the “Subsea Equipment” category. The failure modes included shorts, erratic/high/low/no outputs, spurious operations, faulty signals, and control failures. Since no distinction was made between software failures or hardware failures, ORNL concluded that the reported failures may have resulted from any combination of hardware, software, or hardware and software.

For telephone network systems, a study of sources of system failures and their duration found software errors to have caused less system downtime (in customer minutes, the number of customers affected multiplied by the outage duration in minutes) than any other source of failure except vandalism. Failure modes identified during the ORNL review of the telephone industry were more correctly termed failure mechanisms and included software failures, human errors, external events (i.e., acts of nature), and overloads.

According to a rail industry source reviewed by the ORNL study, the U.S. rail industry is very conservative, and while its standard control systems are primarily digital-based, its vital logic systems use well-proven but antiquated technology (e.g., relays developed in the 1930s). The dispatching systems are not vital systems, and although they provide some checks, the safety functions rely on the vital control logic, which is based on non-digital technology. Information concerning DI&C failures, therefore, was very limited

Conclusions drawn from the non-nuclear operating experience reviews validated concerns regarding software-induced CCFs and the need for D3 regulatory guidance; however, the level of detail describing the digital system software failures was not sufficient for determining appropriate combinations of NUREG/CR-6303 diversity attributes.

As a result of the industry survey, ORNL identified 27 sources of reliability data from the nuclear industry and other industries and determined their availability, usefulness, and internet accessibility. ORNL and the NRC staff used a 5-category ranking system (Very High, High, Medium, Low, and Unknown) to evaluate the relative value of the data bases with regard to developing DI&C failure information. The Very High, High, and Medium sources of data are listed in Table 2. The remaining 22 sources were either of low or unknown value. The very high value sources were from the nuclear power industry (the NPRDS and EPIX data) and the telecommunications industry. Some evaluation has been conducted on the NPRDS and EPIX data, however, the telecommunications data has yet to be evaluated.

The ORNL report recommended a more detailed review of both nuclear power industrys DI&C experience and commercially available databases. The product of this detailed review would be a list of failure modes and failure mechanisms by electronic component on the basis of actual operating experience. NRC staff and ORNL should conduct a review of the digital I&C failure information from the EPIX database augmented with information from the commercially available databases (i.e., third-party databases). These databases contain extensive collections of data on electronic components that include information on component failure rates, failure

mode distributions, diagnostic detection capabilities, and common-cause susceptibilities. These databases appear to provide more specific failure modes than merely designating the failure mode as “fails,” which is a frequently used designation. The NRC staff will identify which of the additional sources will be obtained to determine whether the level of detail in the failure data is sufficient for developing NUREG/CR-6303 diversity strategies.

1.6 Research Report, “Instrumentation and Control Digital Systems Failures in Nuclear Power Plants - From LER data

In 2000, RES conducted a special review of Licensee Event Reports (LERs) to determine whether there was sufficient OE that could be used to identify vulnerabilities of digital systems in nuclear power plants and aid in providing focus areas for performing reliability assessments [15]. The report provided a detailed analysis of the failures involving DI&C systems that occurred in the five year period 1994-1998.

The review of LERs revealed that failures were relatively equally divided between system hardware failures, system software failures, and human-system interface (HSI) failures. For the purposes of the assessment, hardware failures were not considered further as their failure criteria revealed no new failure types.

The relative distribution of software failures between requirement errors, development errors, verification and validation errors, logic (i.e. design) errors, and other software related errors (i.e. miscellaneous errors) is shown in Figure 2. Software errors arising from requirements and logic development activities may be classified as specification and design errors. From the data presented in Figure 2, this category constitutes approximately 61% of the software errors evaluated in the study. Software errors arising from V&V and development activities may be classified as translation errors. This category of errors constitutes approximately 33% of the software errors evaluated in the study. The remaining 6% of software errors arose from operation and maintenance activities. The study did not reveal whether the design errors should have been addressed by use of different technologies (e.g., analog versus digital); different approaches within a technology (e.g., transformer-coupled AC instrumentation versus DC-coupled instrumentation); or different architectures (i.e., the arrangement and connection of components).

- Of particular interest in this evaluation is the relative distribution of failures between the three categories described above. Given the relatively broad time frame of the data, one conclusion that could be drawn with regard to developing diversity strategies is that there may be sufficient data already available for determining appropriate diversity attributes when developing a diversity strategy. It is not expected that failures occurring over the next several years will diminish the relative weighting between the specification and design category and the translation category such that new diversity strategies will be required to account for the shift in failure categories. For example, if new failure data indicate that specification and design failures comprise 50% of all failures instead of 61.25%, this would not (and should not) change the emphasis on which diversity attributes should be used in a diversity strategy. This conclusion suggests that, with regard to identifying the appropriate emphasis on the NUREG/CR-6303 diversity attributes for developing diversity strategies, evaluating additional failure data may not provide additional insights in the short term (1 to 3 years); but could be used to validate proposed diversity strategies at the attribute

level. While the quality of current OE data may not be sufficient for determining appropriate diversity criteria within each NUREG/CR-6303 diversity attribute, RES intends to work with the Operating Experience Branch to develop guidelines for identifying root cause failures in DI&C systems.

1.7 Digital System Failures

As part of DI&C research in the area of D3, RES staff used a number of the data sources discussed above to develop a matrix of DI&C failure data from the US nuclear power industry (1987-2006) in order to evaluate trends in digital system failures in US nuclear facilities

Due to data limitations in the content of the available data, (i.e. root cause investigation and analysis of additional systems/components affected), this set of data could not be used to analyze the potential for CCFs in nuclear facilities. Although this data did not identify DI&C failures at the sub-component level, it did provide system-level causes for many of the events. The data can provide common themes and identify some major issues as they relate to DI&C D3 issues and has been used to provide insight into development of D3 interim staff guidance.

In support of collaborative research for DI&C with EPRI, RES provided this data to the Nuclear Energy Institute (NEI) as the sponsor of an EPRI project to review and categorize DI&C failure data and to conduct additional research to analyze the events in this data and other event data identified by EPRI. NEI has committed to provide this analysis to the NRC staff for review under TWG #2 activities supporting developing D3 regulatory guidance. The work is ongoing and is expected to be completed in mid-2008.

1.8 Quality of Digital System Failure Data

The sources of data listed above have provided useful insights into the relative distribution of failures between hardware and software components in digital systems and validated the potential for CCFs. However, the level of detail in the failure data is such that correlating the software-related failure data to the NUREG/CR-6303 diversity attributes and associated attribute criteria is not currently feasible. Consequently, additional research is being performed to further investigate the failure data provided in the data sources identified by ORNL (see section 1.6 above). Additionally, the results of the EPRI research described in section 1.7 above may reveal additional information that can be used to develop diversity strategies. The NRC intends to work collaboratively with EPRI and the nuclear industry to determine the level of detail required for DI&C root cause analyses. These potential future activities are discussed further in this assessment report's conclusions and recommendations.

II. SYSTEM CLASSIFICATION WITH RESPECT TO COMMON CAUSE FAILURES

In the September 2007 preliminary assessment [1], RES reviewed DI&C classification and categorization methodologies and proposed a strategy that could be used for evaluation and interpretation of digital system operational experience and to support and inform development of on-going digital system regulatory guidance. This section describes how the change from analog technology to digital technology impacts system characteristics and interactions, and how these system characteristics and interactions relate to a digital system classification

structure. This section concludes with a description of a digital system classification structure that supports DI&C OE evaluations and identification of appropriate diversity approaches relative to systems under consideration.

NUREG/CR-6268, Rev. 1 [10], provided a classification system on the basis of intrinsic and extrinsic dependencies. In this classification system, dependencies are first categorized based on whether they stem from intended intrinsic functional and physical characteristics of the system or are due to external factors and unintended characteristics.

Intrinsic dependency refers to cases where the functional status of one component is affected by the functional status of another component. These types of dependencies normally stem from the way the system is designed to perform its intended function. There are several sub-classes of intrinsic dependencies depending on the type of influence that components have on each other.

Extrinsic dependency refers to cases where the dependency or coupling is not inherent or intended in the functional characteristics of the system. The source and mechanism of such dependencies are often external to the system. Examples of extrinsic dependencies are:

- Physical/Environmental. Physical/ environmental dependency is caused by common environmental factors. Environmental factors include harsh or abnormal environments created by a component. For example, high vibration induced by A causes B to fail.
- Human Interaction. Human Interaction dependency is caused by man-machine interaction (e.g., multiple component failure due to the same maintenance error).

NUREG/CR-4780, "Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Procedural Framework and Examples" [16], states that CCFs result from the coexistence of two main factors: (1) a susceptibility for components to fail or become unavailable because of a particular root cause, and (2) a coupling factor or mechanism that creates the condition for multiple components to be affected by the same cause. An example is two pressure relief valves that fail to open because the set-points are set too high. The susceptibility of a system of components to dependent failures compared with independent failures is determined by coupling factors.

The major difference between current plant control system designs and new plant control system designs is that current plants typically use analog-based control technology for safety functions implemented in redundant hardware-based channels that operate independently of one another from process sensor to actuated device; whereas new plant designs propose using digital-based technology that shares data between otherwise independent channels, such that an instrument failure in one channel that is not screened out by fault detection processes can affect the other channels.

In analog-based systems, safety functions are loosely coupled (i.e., their intrinsic dependency is minimized) by virtue of their hardware-based architecture. An 'equivalent' digital-based system that performs the same safety functions may be tightly coupled (i.e., the functional intrinsic dependency may be significantly higher) because all the logical functions are implemented in a single logical construct. For example, digital system designs have been proposed in which different safety systems (e.g., the reactor trip system and the engineered safety features actuation system) may be integrated into a single software program. This merging of

traditionally independent safety systems introduces the possibility that a failure in one safety system (e.g., the reactor trip system) could adversely affect another safety system (e.g., the engineered safety features actuation system). This degree of integration and corresponding vulnerability to failures outside the system is not considered in the design bases for analog hardware-based systems. Differences in coupling between current safety system designs and new safety system designs may become more extreme as new control technologies are introduced in next generation plant designs. For example, a future plant design that relies of semi-autonomous controls could be so tightly coupled that a single defect that leads to a failure could affect multiple safety systems in unanticipated ways.

Current operating plant designs and proposed new plant designs are similar enough that classification of equipment and systems appears, on the surface, to be relatively straight forward. The safety system functions and systems are similar in both plant classes with respect to safety objectives (e.g., reactor trip, containment isolation, actuation of emergency core cooling systems, etc.). However, the means by which these functions are implemented in new plant designs may be different from the traditional safety system designs in current plant designs. For example, new plant designs propose combining safety-related controls and nonsafety-related controls in a single human-machine interface (HMI) such as a touch screen monitor. This technology-supported capability is not used in current operating plants.

The classification structure must be flexible enough to support the underlying analytical tools needed for identifying defects that can lead to failures. The basis of this requirement for tools is the necessity for assigning quantitative values to the data that can be used to determine the relative worth of different diversity strategies for avoiding or mitigating CCFs.

In addition to classifying systems according to intrinsic and extrinsic dependencies, the effect system errors have on the system and dependent systems must also be evaluated. Root cause analysis and statistical growth modeling (e.g. S-curves) are useful in the analysis of software defects. Root cause analysis can provide extensive details on defects; however, the process can require a substantial investment of resources for completion. Root cause analysis requires detailed information on the cause of the errors, which places a burden on the organization to analyze failures at the defect-level (e.g., reviewing software code to identify the cause of software errors and reviewing system development processes to identify deficiencies in software quality assurance processes, activities, and tasks). Growth modeling, on the other hand, is useful for identifying trends in the occurrence of defects and failures, but is not capable of identifying corrective actions due to the inadequate capture of the specific details behind the defects. Therefore, for developing diversity strategies that address the appropriate diversity attributes on the basis of failure history, root cause analysis is a better approach than statistical growth modeling.

To address classification of both systems and failures, the NRC staff intends to use a digital system classification strategy consisting of three attributes of digital systems. This classification method is similar to the method used by the COMPSIS project to classify systems and failures (see section 1.3, above). The first attribute, digital system complexity, addresses intrinsic interactions between digital system hardware, software and firmware (e.g., communication between different components, multi-tasking, etc.), and an overall digital system size and complexity index. The size and complexity index could be a function point or cyclomatic complexity metric. This first attribute will represent how critical intrinsic interactions and system

complexity are incorporated onto a fault free model of a digital system. Potential sub-attributes of the digital system complexity attribute include:

- Design Complexity
- Software Complexity
- Hardware Complexity
- System Function Complexity
- System Testability
- Kind and amount of testing
- Self-test and diagnostics

The digital system complexity attribute would range from “simple” to “complex”.

The second attribute, digital system interactions/inter-conductivity, addresses extrinsic interactions (interactions between the digital system and the plant physical processes). The attribute measure would represent how the digital system under study interacts with other systems and process parameters within the plant and how important accurately assessing these interactions are to the system safety. Digital systems that are loosely coupled and/or have very few extrinsic interactions would not interact dynamically with the overall plant and would have a low interactions/inter-connectivity score. Potential sub-attributes of digital system extrinsic inter-connectivity include:

- Number and types of inputs and outputs
- Inter-system communications
- The importance of timing of events in system communication
- System feedback with other systems

The digital system inter-connectivity attribute would range from “loosely coupled” to “tightly coupled.”

The third attribute is digital system importance. This attribute measure represents both traditional risk important measures, such as component risk achievement worth, and how important the system is for maintaining defense-in-depth concepts. This measure could be implemented by use of a plant integrated decision making panel similar to what is currently done to determine if a system is included in the NRC maintenance rule’s (a) 4 requirements. It should be noted that because many of the digital systems included in this effort have significant extrinsic interactions (i.e., will score high on the system interactions/inter-connectivity attribute) these systems may not be accurately represented in current PRA models, so the information associated with their risk importance measure may need to be adjusted accordingly. The current PRA methodology may need to be modified to support the development of an accurate risk importance measure for digital systems. Potential sub-attributes of digital system importance include:

- Attributes of system importance are associated with system operations
- System Function (reactor trip, control, etc.)
- Back-up functions for another system
- Errors in the system affecting other systems
- System importance to risk (F-V, RAW, etc.)

The digital system importance attribute would range from “low” to “high.”

This classification structure will be used to support evaluation and interpretation of digital system operational experience (e.g... evaluate whether the data indicate that digital system failure rates are related to system complexity). The classification structure also will support development of regulatory guidance on digital system designs based on the categorization attributes.

For evaluating current and proposed regulatory guidance in the area of DI&C D3 assessments, the most important attributes of the proposed classification structure will be system complexity and system inter-connectivity. These attributes should capture the likelihood of system CCFs and the likelihood that the CCFs could affect multiple systems. Currently, NRC guidance includes assessment of system diversity in the areas of equipment diversity, human diversity, design diversity software diversity, functional diversity and signal diversity. In D3 evaluations the current equipment, human, design and software diversity criteria can be mapped into the complexity attribute, the signal diversity criteria can be mapped to the inter-connectivity attribute, and the functional diversity criteria can be mapped to the importance attribute. Current and proposed D3 regulatory guidance provide a method for assessing whether sufficient diversity and defense-in-depth exists in a design. The proposed classification structure could be used to determine that a system is sufficiently simple to ensure the likelihood of common cause failure is small, that the system interconnectivities are sufficiently isolated to ensure a low likelihood of propagation of a failure; there is sufficient diversity that any component failure will have little effect on the system’s safety function (importance), or that additional diversity is required to avoid or mitigate potential CCFs.

To date, the nuclear industry has implemented a number of nuclear plant systems using digital technology. Most of these plant systems are not safety-related (e.g., feedwater systems and turbine governors). Digital safety-related systems, on the other hand, have not been implemented in sufficient number to allow development of an extensive database of safety applications. Some safety systems (e.g., emergency load sequencing systems and emergency feedwater systems) have been implemented; however, digital reactor trip systems and engineered safety feature systems have not been installed in currently operating plants. Safety systems for new reactor designs almost certainly will be implemented with some form of digital technology (e.g., microprocessor-based or programmable logic-based); however, these systems are in the conceptual phase of development. Consequently, because of the low number of digital safety systems in current operating plants and the conceptual state of safety system designs in new reactor designs, an extensive inventory of digital systems in which the proposed classification structure has been implemented has yet to be developed.

III. CONCLUSIONS

Operating Experience Evaluation

The assessment found that detailed root cause information on DI&C failures is difficult to obtain for several reasons. The process of performing root cause analysis, the cost of performing the analysis, and the willingness of end users to participate in a data collection effort all impede gathering sufficiently detailed information. This is especially the case for failures that are

relatively inexpensive to remediate, such as replacement of an inexpensive component. It is not uncommon for failure reports to state the cause of a failure is a “software” failure, instead of identifying the specific cause of the software failure; such as incorrect specification, operator error on rebooting system, etc. If the consequences of a failure are not severe (e.g., temporary loss of availability), a root cause analysis may not be detailed enough to be useful for developing specific diversity strategies.

The effort to develop detailed root cause analysis information is further compounded by the relatively rapid pace at which digital technology advances are introduced into industrial process control systems. The short lifetime of each generation of digital equipment limits the base of experience available for diagnosing model-specific failures, and can lead to systems consisting of different generations of equipment and software. This continual onset of obsolescence can limit the amount of experience that can be gained from the use of a specific component or application over a longer period, thereby diminishing the ability to perform effective root cause analyses.

Continual obsolescence affecting the quality of failure information has a similar element in the software (i.e., logical construct) component of digital systems because software modifications to improve system capabilities are fairly common in new systems during the initial phase of their introduction into the process systems they are to control. Additionally, the ease with which software may be modified to incorporate new functionality effectively degrades the base of experience developed through use of the previous version of the software. Consequently, as the software evolves from the initial version to later versions, the ability to identify specific root causes of failures becomes more difficult. Also software system development personnel change frequently enough that, over a relatively short period of time, system expertise becomes the responsibility of personnel who were not involved in the original development of the system.

The assessments of DI&C failure data and OE indicate that there is limited availability of high-quality data. Detailed causal data is particularly difficult to locate. Analysis is also difficult due to inconsistencies in failure category definitions. Although additional research was recommended to specifically identify the failure modes and causes of failures in DI&C systems, the assessment findings to date validate concerns that software-induced CCFs are credible events. This is evident by the numerous examples of software failures that were found during reviews of the various data sources mentioned in this report.

On-going programs such as the NRC OE Program and the COMPSIS project are valuable in that they collect, analyze and distribute information, thereby providing lessons learned to applicants, vendors, and licensees. Additionally, the COMPSIS project has developed a classification system to support consistent failure data input and categorization for subsequent data analysis. Ongoing NRC OE programs can be helpful in providing insights on regulatory guidance addressing D3 of digital systems in the nuclear industry. The failure data bases identified in Section I must contain data that is detailed enough to be correlated to the diversity attributes identified in NUREG/CR-6303 in order to evaluate the relative worth of different diversity strategies. For example, if the failure rates of functional approaches are higher than the failure rates of specific equipment components, a diversity strategy that weights functional approaches more importantly than approaches emphasizing the use of diverse equipment would be warranted. However, to date these sources of failure data have not been of sufficient detail for developing NUREG/CR-6303 diversity strategies.

With regard to developing NUREG/CR-6303 diversity strategies, it is expected that failures in digital systems occurring over the next several years will provide only relatively insignificant changes in the current weighting between the diversity strategy attributes. For example, if new failure data indicate that requirements-related failures (which can be subdivided into NUREG/CR-6303 design and function attribute failures) comprise 50% of all failures instead of 61.25% of all digital system failures (as shown in Figure 2), this would not (and should not) change the emphasis on which diversity attributes should be used in a diversity strategy. However, as new technologies are introduced into nuclear industry safety system designs, new failure data may prove valuable for determining diversity strategies for these new systems.

Classification and Inventory of DI&C Systems

The issues with quality of root cause analyses may be addressed through the implementation of technology-independent processes for performing root cause analyses of failures. Consequently, a system classification process may be used as the entry criteria for selecting a specific diversity strategy. For example, systems that are highly coupled will require more stringent diversity strategies because the likelihood of a CCF causing a cascading failure or system failure is higher. In Section II, DI&C system classification structure attributes and how the attributes relate to D3 strategy development were discussed. A classification structure was selected and will be used to support developing an inventory of DI&C systems as these systems are selected for upgrades in operating reactors and for DI&C systems in new reactors.

Recommendations:

RES has evaluated sources of operating experience with digital systems in the nuclear and other industries to obtain insights regarding potential failure modes. Based on the insights obtained and the current direction of D3 strategy development, there are no recommended changes for D3 regulatory guidance at this point. However, RES intends to review of additional non-nuclear sources and improving support of the ongoing nuclear operating experience reviews to obtain more detailed information on the NUREG/CR-6303 diversity attributes and associated attribute criteria to be addressed in proposed diversity strategies.

- RES intends to obtain the high value non-nuclear data sources identified in Table 2 and review this data for additional insights.
- RES intends to work with the Operating Experience Branch to develop guidelines for identifying root cause failures in DI&C systems.
- RES intends to work with the Operational Experience TRG for Instrumentation and Controls to augment DI&C operational experience reviews using system classification methods.

RES has evaluated DI&C inventory and classification systems that could be used for the various types of digital hardware and software systems that are being used and are likely to be used in nuclear power plants. RES supports the COMPSIS DI&C system classification structure for DI&C failure data capture. Further, a classification system for use in operational experience reviews and D3 regulatory guidance should be developed and maintained. A DI&C system inventory has not yet been developed due to lack of detailed digital system classification information, the scarcity of digital safety system upgrades in operating reactors, and the conceptual design development state of new reactor DI&C safety system designs.

- RES intends to develop an inventory of digital systems as new digital systems are introduced into the nuclear industry. The system inventory will be structured to align with the system classification based on specific vendor designs consistent with the method described in this report.

References:

1. U.S. Nuclear Regulatory Commission, *NRC Digital System Research Plan, FY 2005 – FY 2009*, (ML061150050), April 26, 2006.
2. U.S. Nuclear Regulatory Commission, *Preliminary Assessment of Major Issues or Common Themes in Inventory and Classification and Operating Experience Evaluation for Digital I&C System*, (ML072710480), October 1, 2007.
3. Code of Federal Regulation, Title 10, "Energy", Part 50, "Domestic Licensing of Production and Utilization Facilities"
4. U.S. Nuclear Regulatory Commission, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, (ML071790509) December 1994
5. Office of Nuclear Regulatory Research Job Control Number N6176, *Diversity and Defense-in-Depth Design Techniques in Nuclear Power Plants*.
6. *Summary of October 19, 2006, Meeting With NEI And Nuclear Power Industries Regarding Instrumentation And Control Technical Issues*, (ML063060583), November 3, 2006.
7. Oak Ridge National Laboratory, K. Korsah, M. D. Muhlheim and D. E. Holcomb, *Industry Survey of Digital I&C Failures*, December 2006.
8. U.S. Nuclear Regulatory Commission, Memorandum from J. E. Dyer, Director, Office of Nuclear Reactor Regulation, and Carl J Paperiello, Director, Office of Nuclear Regulatory Research, "*Request For Support In Implementing The New Agency Reactor Operating Experience Program*", (ML050970097) July 1, 2005
9. U.S. Nuclear Regulatory Commission, *Reactor Operating Experience Program*, NRC Management Directive 8.7 (ML062970023), September 28, 2006.
10. Nuclear Regulatory Commission, *Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding*, NUREG/CR-6268, Rev. 1, (ML072970404) September 2007.
11. Organization for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA), Committee on the Safety of Nuclear Installations, *COMPSIS, OECD Exchange of Operating Experience Concerning COMPuterised Systems Important to Safety at NPPs, Event Coding Guidelines*, V 3.0, November 23, 2006.
12. Institute of Nuclear Energy Research, Republic of China, *Qualitative Analysis of COMPSIS Events*, October 17, 2007.
13. Institute Of Nuclear Power Operations, *Memorandum of agreement between the Institute Of Nuclear Power Operations and the U. S. Nuclear Regulatory Commission*, November 14, 2005.
14. Nuclear Regulatory Commission, *Completion of Reliability And Availability Data System, Version 1.0*, April 18, 2001 (ML003759591)
15. R. Brill, "*Instrumentation and Control System Failures in Nuclear Power Plants*," Proceedings of the International Symposium on Software Reliability Engineering, 2000.
16. U.S. Nuclear Regulatory Commission, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Procedural Framework and Examples*, NUREG/CR-4780, (ML070570105), January 1988.

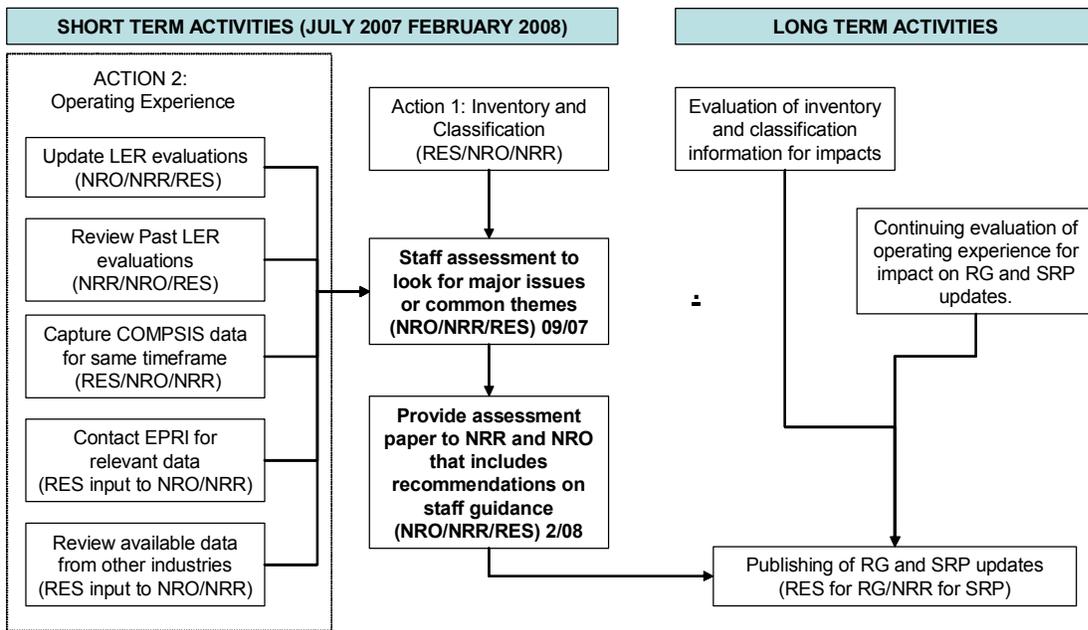


Figure 1. Operational Experience Assessment Process

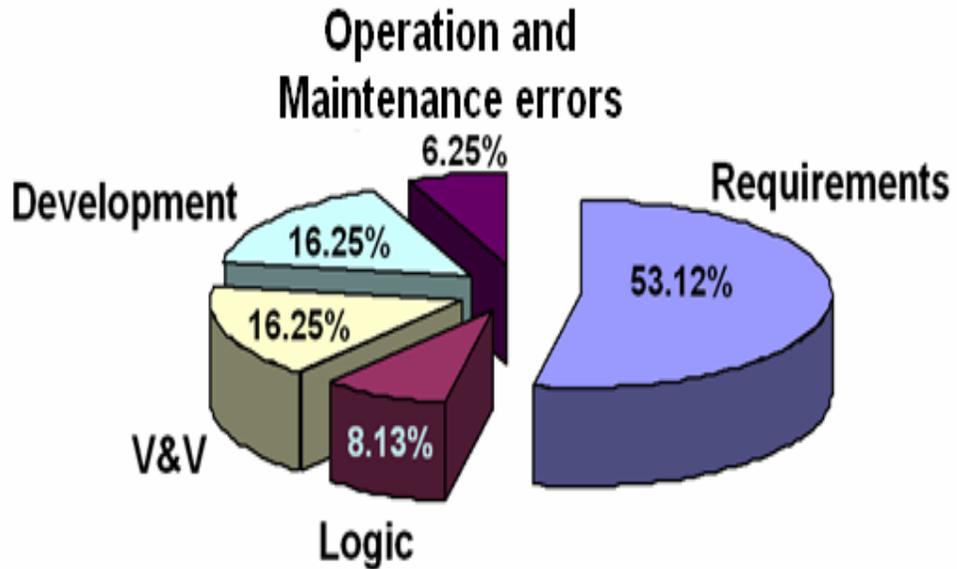


Figure 2. Total Software Errors as defined by percentage

Table 1. AEC failure categories compared to NUREG/CR-6303 diversity attributes

AEC Failure Categories	NUREG/CR-6303 Diversity Attributes
Design	Design, Function, Signal, Software
Hardware Failures	Equipment, Signal
Communication	Function, Signal
Quality assurance (QA)	Human (Life Cycle Process)
Configuration management	Human (Life Cycle Process)
Human factors	Design
Routine maintenance	Human (Life Cycle Process)

No.	Database	Industry	Availability	Usefulness	Value
1	<i>Reliability, Maintainability, and Risk: Practical Methods for Engineers</i> , 6th edition (D. J. Smith)	Telecomm.	Book \$62.95, database £499	Both the book and database provide information on microelectronics. The value of the information contained in the database is currently unknown however it is likely to be a valuable source because it appears to be focused on microelectronics. http://www.maint2k.com/failure-rate-data-in-perspective.htm	VERY HIGH Contains data from many sources
2	<i>Nuclear Plant Reliability Data Systems (NPRDS) and Equipment Performance and Information Exchange (EPIX)</i> , INPO	Nuclear power		In the late-1990s, INPO created EPIX to replace NPRDS; EPIX provides an industry-wide database of information on Maintenance Rule components at all U.S. nuclear power plants. Useful data is contained in the database however access requires INPO membership (utility) or NRC permission, and an operating experience review complete with associated report would be required to make use of the raw data. The EPIX system, however, is not particularly well suited for more extensive event analysis-these capabilities are simply not present with the Web-based interface that is currently used for the EPIX database queries. For instance, it is not able to display event trends or to use statistical functions to identify outliers. ORNL has developed and utilized a system that permits the detailed EPIX data to be used for detailed analyses, including trending and outlier analyses, in both tabular and graphical formats, in support of NRC projects. The system has been used to identify potential degradation of passive components that was the subject of a recent NRC-sponsored study.	VERY HIGH NRC has access

Table 2. Value of Reliability Data Bases (cont)					
No.	Database	Industry	Availability	Usefulness	Value
3	<i>Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2006 Edition</i>	Petrochemical	\$485 + shipping	This report provides reliability data estimates for components of control and safety systems. Data dossiers for field devices (sensors, valves) and control logic (electronics) are presented. Control and safety system vendors participated in producing this data handbook. The value of the information contained in the data handbook is currently unknown; however it is likely to be a valuable source because it appears to cover I&C components and specifically identifies failure modes. http://www.sydvest.com/Products/pds-data/	HIGH recommend
4	<i>SPIDR— System and Part Integrated Data Source</i>	Generic	\$1995	This database contains reliability data on both commercial and military electronic components for use in reliability analyses and contains failure data on ICs, discrete semiconductors, resistors, capacitors, and inductors/transformers. SPIDR™ replaces the following reliability data resources: <ul style="list-style-type: none"> • <i>Nonelectronic Part Reliability Data</i> (NPRD-95), • <i>Electronic Part Reliability Data</i> (EPRD-97), • <i>Failure Mode and Mechanism Distributions</i> (FMD-97), and • <i>Electrostatic Discharge Susceptibility Data 1995</i> (VZAP) The value of the information is currently unknown, however it appears to be a valuable source of information on the failure modes of ICs. http://src.alionscience.com/spidr/	HIGH Contains data from many sources
5	<i>Guidelines for Process Equipment Reliability Data, with Data Table, AICHE</i>	Petrochemical	\$29/year Book \$119	The book supplements <i>Guidelines for Chemical Process Quantitative Risk Analysis</i> by providing the failure rate data needed to perform a chemical process quantitative risk analysis. http://www.aiche.org/Publications/pubcat/listings/0816904227.aspx	MEDIUM Book would be good value