

Program Title: Emerging Technologies Research Program
Document Title: Industry Survey of Digital I&C Failures
Document Type: Letter Report
Authors: K. Korsah, M. D. Muhlheim and D. E. Holcomb
NRC Manager: Tolani Owusu
ORNL Manager: Kofi Korsah

Prepared for
U.S. Nuclear Regulatory Commission
Under
DOE Interagency Agreement 1886-N640-9W
NRC JCN No. Y6409

Prepared by the
Nuclear Science and Technology Division
OAK RIDGE NATIONAL LABORATORY
P.O. Box 2008
Oak Ridge, Tennessee 38731-6285
managed by UT-Battelle, LLC
For the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

December 2006

Notice

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

TABLE OF CONTENTS

Title	Page
SUMMARY	1
1. INTRODUCTION	3
2. DIGITAL SYSTEM FAILURE MODES AND SOURCES OF FAILURE RATE INFORMATION.....	4
2.1. The Benefits of and Issues with Digital Technology in Safety- Critical Applications	4
2.2. Computer System Failures: A Brief Review	4
2.2.1. Sources of Failure Rate Information	4
2.2.2. Computer Hardware Failures.....	8
2.2.3. Software Failures.....	10
2.2.4. Systematic Faults	11
3. DIGITAL I&C FAILURES IN THE PETROCHEMICAL INDUSTRY.....	12
3.1. Offshore Reliability Data	12
3.1.1. Control and Safety Equipment Category	12
3.1.2. Control Systems in Subsea Equipment Category.....	13
4. DIGITAL I&C FAILURES IN THE AVIATION INDUSTRY.....	17
4.1. Introduction	17
4.2. The Aviation Safety Information Analysis and Sharing (ASIAS) System.....	17
5. FAILURES IN THE PUBLIC TELEPHONE NETWORK	21
5.1. Reasons for Investigating Failures in the Telephone Network.....	21
5.2. Results of Literature Review	21
6. DIGITAL I&C FAILURES IN DOMESTIC NUCLEAR POWER PLANTS.....	24
6.1. Introduction	24
6.2. Some Failure Rate Information for Gen III Plants	24
6.2.1. Lungmen, a GE ABWR.....	24
6.2.2. GE ESBWR.....	25
6.2.3. AP600 and AP1000.....	26
6.2.4. ACR-700.....	27
7. CONCLUSIONS AND RECOMMENDATIONS.	29
8. REFERENCES	31

SUMMARY

This *Industry Survey of Digital I&C Failures* document reports on the results of a survey of available sources of digital instrumentation and control (I&C) failures in nuclear and nonnuclear industries, with a focus on the latter. Failure data that could be obtained for review included the *Aviation Safety Information Analysis and Sharing (ASIAS)* System and the *Offshore Reliability Data (OREDA)* system.

The ASIAS system was searched for digital-instrumentation-related incidents^a. The total number of reports in the database was 86,682, which represents data from 1978 to present. From these reports, 67 incidents were identified as computer-related. Based on this data, the number of aircraft, and the availability of that aircraft,^b a computer failure rate in the commercial aviation industry was estimated to be $2.0 \times 10^{-7}/h$. Because the reporting system is voluntary, this value represents a lower bound estimate.

Most of the available offshore reliability data dealt with mechanical and electromechanical equipment. Because the focus of this study is on digital I&C equipment, only the small subset of the data that was I&C-related was analyzed. This included the “Control and Safety Equipment” category as well as the control systems in the “Subsea Equipment” category. Failure rates ranged from $3 \times 10^{-8}/h$ to $1.1 \times 10^{-6}/h$.

We also reviewed available literature on I&C failures in the public telephone networks. Although telephone systems are not necessarily considered failure-critical, they were nevertheless reviewed because telephone switch manufacturers are among the world’s leaders in computing technology. They dedicate a significant amount of research on developing highly reliable systems, and their software development processes typically incorporate the most sophisticated practices, supplemented by elaborate quality assurance functions. Telephone switching tasks also require some of the most complex and sophisticated computing systems in existence. For example, software for a switch with even a relatively small set of features may comprise several million lines of code. One interesting finding from the literature review of the telephone network failures was that despite the digital complexity of the system, software errors caused less system downtime (2%) than any other source of failure except vandalism. The effect of hardware and software failures were similar in terms of the average number of customers affected (96,000 and 118,000) and the duration of the outage (160 and 119 minutes for hardware and software failures, respectively).

Although the scope of this review originally included the train/rail industry, no information could be obtained for it. Several contacts and futile attempts were made to obtain relevant information in the rail sector. One industry expert acknowledged that such digital I&C databases exist in the train/rail industry, but that they could not be released for public use. Another industry source was rather doubtful that such databases for the train/rail systems exist, and even if they existed at all, doubted that it would be useful to this task. According to this industry source, the U.S. rail industry is very conservative, and its vital logic uses 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 field logic, which is based on hardware.

Finally, we briefly reviewed failure data used in probabilistic risk assessments (PRAs) for Generation III (Gen III) nuclear power plants. Gen III plants were selected for this review because the PRAs for these plants are expected to use the most recent, up-to-date failure data. Failure rates for microprocessor based

^a That is, occurrences that did not involve fatalities (accidents).

^b The reader is cautioned that this is only a rough estimate based on data we were able to assemble in the relatively short period of this study. Some assumptions were also made which, although we believe are conservative, may need to be adjusted after a more detailed study.

components and discrete logic components were found to vary between $5 \times 10^{-6}/\text{h}$ and $1.0 \times 10^{-5}/\text{h}$. The probability of failure on demand for solid-state components were found to range from 2.8×10^{-5} to 9×10^{-4} . The probability of failure of the solid state components are typically based on the assumption that 95% of the component failures will be detected by self-testing, performed every 30 min. It is also assumed that the remaining 5% will be detected only during surveillance tests performed quarterly (every 2190 h). In both cases, the mean-time-to-repair is 5 hours.

This brief study indicates that digital I&C failure rates used in the safety assessments in the failure-critical nonnuclear industries are lower than for nuclear power plants. It is recommended that a more detailed study be performed to substantiate this or to determine whether the comparisons are appropriate or not.

It is also recommended that this study be expanded to perform a more detailed review of both the nuclear power industry's digital I&C experience and the commercially available databases. With respect to the nuclear power industry, many PRAs cite 25-year old reports for data and supplement that with recent (internal) studies for I&C components. The product of this detailed review would be a list of failure rates by electronic component. This data would be supplemented with failure modes identified from actual operating experience through a review of the digital I&C failure information from the EPIX database. Information from the commercially available databases (i.e., third-party databases) would complete the review. These databases appear to 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.

1. INTRODUCTION

There are 104 fully licensed nuclear power reactors in the United States,¹ although one is not currently operating.^a At present there are also four certified new reactor designs—AP600, AP1000, CE80+, and ABWR, with several other designs in the precertification or certification stage. In addition, the U.S. Department of Energy (DOE) actively participates in the Generation IV International Forum (GIF) that seeks to develop the next generation of commercial nuclear reactor designs before 2030.^{2,3} The instrumentation and control (I&C) of all these generations of nuclear power plants, including upgrades of current generation of plants (i.e., Gen II), are expected to make extensive use of digital I&C. Some of the issues that an increased application of digital I&C in safety systems pose are (1) the possibility of increased failures due to software or embedded firmware that could compromise plant safety and (2) the probability of common cause failure due to software errors.

The Nuclear Regulatory Commission (NRC) initiated this task, “Industry Survey for Digital I&C Failures,” within the Emerging Technologies project to investigate digital I&C failures in some safety-critical systems and to document its failure modes and occurrence frequencies. In particular, this task was to survey the nuclear and nonnuclear industries for available sources of digital I&C failures, with a focus on the latter. The industry sources were to include but were not limited to: the Federal Aviation Administration (FAA), train/rail systems, and petrochemical plants. Access to these data was to be investigated. Any obtained data were to be categorized according to their failure mechanisms. Licensee event reports (LERs) and other NRC-related databases were not to be used for this survey.

This letter report documents the findings from that task.

^aBrown’s Ferry 1, the nonoperating reactor [owned by Tennessee Valley Authority (TVA)], has been shut down since 1985. TVA has plans to restart the reactor in 2007.

2. DIGITAL SYSTEM FAILURE MODES AND SOURCES OF FAILURE RATE INFORMATION

2.1. The Benefits of and Issues with Digital Technology in Safety-Critical Applications

Digital technology has proliferated in several commercial and safety-critical application areas. Examples include the petrochemical industry, medical I&C, high-speed surface and air transportation, and food processing. The reasons for this proliferation are many, the most significant of which include (1) the ability to pack several complex and diagnostics functions into a small volume [i.e., an integrated circuit (IC)]; (2) the greater precision digital systems offer over their analog counterparts; (3) the ease of adaptability and modification (e.g., simply by loading a different program); and (4) the ease of multiplexing, which considerably simplifies cabling. However, digital systems are also seen as having issues associated with their use, and NRC is understandably cautious in allowing its “wholesale” application in nuclear power plants. These issues include (1) new failure modes, especially the potential for common-cause failures; (2) increased complexity, which reduces the likelihood that the system can be exhaustively tested, therefore making it difficult to prove system safety; and (3) sensitivity to the environment, including temperature, humidity, static electricity and electromagnetic interference/radio-frequency interference (EMI/RFI). While some of these issues are being resolved through NRC-sponsored confirmatory research^{4,5,6,7} and through interactions with the international community, digital system reliability and software validation remain significant issues. This *Industry Survey for Digital I&C Failures* task was initiated by the NRC to gain some insight into digital systems’ long-term performance and failure modes in safety-critical applications.

2.2. Computer System Failures: A Brief Review

Computer system failures may arise from one of three categories: (1) hardware faults, (2) software faults, and (3) systematic faults. Some data sources (e.g., IEC^a 61508) identify only two types of faults: “random” hardware faults and systematic faults. Other data sources identify software faults as a separate category. In this overview, software will be treated as a separate category.

For the purposes of discussing computer system failures, Figure 1 is used to depict a generalized computer system. It could represent an embedded microcontroller (the simplest computer structure from a block diagram point of view), in which case the operator block in the diagram may be assumed to be eliminated. The figure could also represent one computer subsystem within a distributed computer system.

The ability to properly analyze the performance of a system requires data on all the components. Although the actual failure data are difficult to obtain, the calculated failure rates based on that data (and in some cases the underlying assumptions) are available.

2.2.1. Sources of Failure Rate Information

Component failure rates and failure modes are generally available or can be calculated using several sources. These include (1) vendor data, (2) technical literature, (3) facility records, (4) published or private databases, and (5) reliability prediction models..

^aInternational Electrotechnical Commission

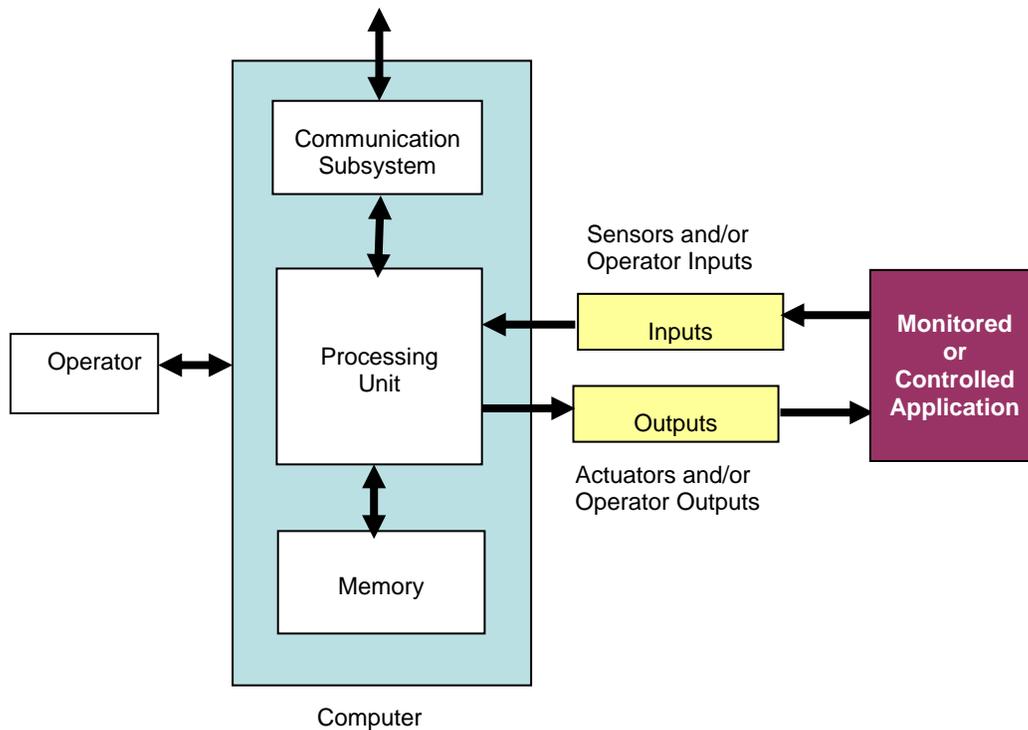


Figure 1. Generalized computer system in a power plant environment

Vendor Records

Vendors seldom provide proprietary failure data because doing so could place them at a competitive disadvantage. However, even if vendor failure data are available, the data generally do not take into consideration actual process or environmental factors and history.

Technical Literature

A good understanding of how faults are introduced into software as a result of programmer mistakes and oversights can be obtained from technical literature covering software reliability and engineering. In addition, software faults and failures are addressed in risk and reliability studies. However, although the level of knowledge is increasing rapidly, the ability to evaluate software failures and any resulting effects is still in its infancy compared to the ability to evaluate hardware failures.

Facility Maintenance Records

Digital equipment failure data may be available in facility maintenance and operating records. However, depending on service history, failure mode data from this source may not include all possible component failure modes. Many nuclear power plants maintain maintenance records and use them to provide plant-specific information for their probabilistic risk assessments (PRAs). The failure rates could be obtained from the plant-specific PRAs. However, licensees do not provide the failure data in their PRAs, and not all licensees provide the failure rates. Licensees do voluntarily report problems with nuclear plant

equipment and systems to the Equipment Performance and Information Exchange (EPIX) system, operated by the Institute of Nuclear Power Operation (INPO).

Third-Party Databases

There are commercially available databases that provide failure rate information in the form of handbooks, standards, and electronic databases. In addition, several agencies have collected failure rate information from publicly available sources. A sampling of several of the databases is listed below (this list is not, nor is it meant to be, all inclusive).

Petrochemical industry databases

- OREDA-92, *Offshore Reliability Data*, DNV, Hovic, Norway, 2002. The data presented are on maintenance, equipment availability, and safety improvement needs on offshore oil rigs.
- American Institute of Chemical Engineers, Center for Chemical Process Safety, *Guidelines for Process Equipment Reliability Data, with Data Tables*, 1989.
- *Safety Equipment Reliability Handbook*, exida.com, 2003. This handbook is intended to supply safety integrity verification information for equipment used in industrial process safety protection applications (i.e., sensors, logic units, actuators). The equipment included is used primarily in the process and machine industries. The handbook provides failure rates, failure mode distributions, diagnostic detection capability, and common-cause susceptibility.

Telecommunication databases

- D. J. Smith, *Reliability, Maintainability, and Risk: Practical Methods for Engineers*, 6th edition, Butterworth-Heinemann, 2001. The appendices in this book provide general failure rates for hardware and for microelectronics. It compares the microelectronics failure rates for a range of temperature and device complexities to MIL-HDBK-217E; British Telecom HRD4; French PPT CNET databank; and some field data collected by the author. The full database is available in FARADIP.THREE (FAilure RATE Data In Perspective).
- HRD5, *Handbook of Reliability Data for Electronic Components Used in Telecommunications Systems*, developed by British Telecommunications plc., 1994. This document is a collection of field data by British Telecom's Laboratories at Martlesham Heath. It lists failure rates for ICs, discrete semiconductors, capacitors, resistors, electromechanical and wound components, optoelectronics, surge protection, switches, visual devices and miscellaneous components (e.g., microwave). The failure rates obtained from this document are generally optimistic compared with the other sources, often by as much as an order of magnitude. This is because of its 'screening' of the data whereby failures that can be attributed to a specific cause are eliminated from the data once remedial action has been introduced into the manufacturing process. Considerable effort is also directed towards eliminating maintenance-induced failures from the data.

Generic databases

- ISA-TR84.00.02-2002, Parts 1–5, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*.
- SPIDR—*System and Part Integrated Data Source*, is a comprehensive database of reliability and test data for systems and components by the Alicon System Reliability Center (SRC) (formerly Reliability Analysis Center or RAC). SPIDR™ replaces the following RAC reliability data resources: *Nonelectronic Part Reliability Data* (NPRD-95), *Electronic Part Reliability Data*

(EPRD-97), *Failure Mode and Mechanism Distributions* (FMD-97), and *Electrostatic Discharge Susceptibility Data 1995* (VZAP). The *EPRD – Electronic Parts Reliability Data* contains reliability data on both commercial and military electronic components for use in reliability analyses and contains failure rate data on ICs, discrete semiconductors, resistors, capacitors, and inductors/transformers.

- Institute of Electrical and Electronics Engineers (IEEE) Std. 500, *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Components, and Mechanical Equipment Reliability and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*. The data in this standard are based on a combination of reports and estimates of several experts drawn from a cross section of industry, including nuclear, fossil-fueled power, and chemical.⁸

Nuclear power industry databases

- International Atomic Energy Agency (IAEA), *Component Reliability Data for Use in Probabilistic Safety Assessment*, IAEA-TECDOC-478, Vienna, 1988. The IAEA's database consists of ~1000 records on 420 component types compiled from 21 publicly available data sources. The data base includes data for nuclear power plant components typically modeled in PRAs. Failure rates for digital instrumentation are from NUREG/CR-1740.
- *EIREDA European Industry Reliability Data Handbook*, C.E.C.-J.R.C./ICEI 21020 ISPRA (Varese) Italy, EDF-DER/SPT 93206 Saint Denis (Paris) France, 1991. The data provided relates to failures of components that play a role in the safety of EDF nuclear plants (34 units), including failures in relation to maintenance. Components include thermal hydraulic, electric, and electronic equipment and components.
- *T-Book Reliability Data of Components in Nordic Nuclear Plants*, ATV Office, Vallingby, Sweden, 1991. This databank provides failure data for the safety analyses of the Nordic Nuclear Power Plants (14 units). Data is automatically collected from the Computerized Plant Maintenance Systems; reliability parameters are updated with Bayesian techniques.
- INPO, *Nuclear Plant Reliability Data Systems (NPRDS) and Equipment Performance and Information Exchange (EPIX)*. The NPRDS was begun in the mid-1970s by INPO. This database records and analyzes reliability data on specific nuclear equipment and components. 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.
- U.S. NRC, *Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at US Commercial Nuclear Power Plants*, NUREG/CR-1740, Rev. 1, 1984. This report describes a computer-based data file developed from LERs of I&C components in commercial nuclear power plants for the period from January 1, 1976, to December 31, 1981. In addition to the creation of the file, summaries of data contained in the file were made to obtain data for risk assessment and statistical purposes. Gross constant fault (failure and command fault) rates were estimated for major components and channels that provide a direct reactor trip.

Reliability Prediction Models

Reliability prediction models offer standard equations that allow users to calculate the failure rate of components based on component data and parameters. There are several different reliability prediction models available. The model parameters for reliability prediction models for electronic components include production factors (e.g., material selection, design and construction, production maturity, storage conditions, and transport conditions) and application factors (e.g., operating conditions, electrical stress, climatic environment, mechanical stress, and application temperature). Some of the models are listed below.

- MIL-HDBK 217F, Change 2, *Reliability Prediction of Electronic Equipment*, U.S. Department of Defense, February 28, 1995. This handbook was developed for predicting failure rates of electronics and is used to estimate failure rates when the equipment is brand new, has not been built yet, or does not yet have a history of operating in the field. This standard typically provides overly conservative failure rates, sometimes by orders of magnitude. Failure rates are estimated using factors such as quality, temperature, stress levels, environment, generic, learning, and complexity of the component.
- Centre National d'Etudes les Telecommunications (CNET) 93. The CNET 93 reliability standard was developed by France Telecom and provides reliability models for a wide range of components. CNET 93 is a comprehensive model similar to MIL-HDBK-217, in that it consists of regression models for the prediction of component failure rates.
- HRD5, *Handbook of Reliability Data for Electronic Components Used in Telecommunications Systems*, developed by British Telecommunications plc., 1994. This document not only provides failure rates for electronic components, but it also provides models to estimate failure rates for a wide range of components. In general, HRD5 is similar to CNET 93, but provides simpler models and requires fewer data parameters for analysis.
- Bellcore TR-332 (Telcordia SR-332) mean-time-between-failure (MTBF) Calculations. This standard is now known as Telcordia GR-332. Telcordia GR-332 is a reliability prediction standard developed by Bellcore Communications Research (Bellcore) for telecommunications companies, but later adopted by many other organizations. Bellcore, which previously was the telecommunications research arm of the Regional Bell Operating Companies (RBOCs), is now known as Telcordia Technologies. The Bellcore Reliability Prediction Procedure (RPP) document provides mathematical reliability models for nearly all types of electrical and electronic components. These reliability models are based on parameters of the components such as number of transistors, power dissipation, and environmental factors.

2.2.2. Computer Hardware Failures

Digital Integrated Circuits

Table 1 shows typical failure modes for digital ICs, as one would find in FMD-91. If one were to review all available failure mode databases, one will find that all digital ICs can exhibit any or all of the failure modes listed in the table, except for “data bit loss,” which is peculiar to memory devices.⁸ Based on the device construction, failure mechanisms and failure mode data, there are three things that can go wrong:⁸

1. Input data to the IC may be altered between the pins and the chip. The active circuitry (chip) of an IC is in the center of the package encapsulation, with wires connecting from the chip to the IC pins. An open wire (connecting the chip to a pin) might inadvertently contact another wire or a wrong conductor on the chip and cause a short. Even when the open wire does not touch another wire and cause a short, it could prevent a correct bit from reaching the chip.
2. Output data from the IC may also be altered between the pins and the chip. Just as in (a), a short may be caused at an output pin, or data from the IC chip may fail to reach an output pin.
3. The chip itself may fail to perform its intended I/O function. The IC chip consists of thousands to millions of transistors as an integral part of the silicon (chip) material. One or more transistors, as well as one or more circuit paths, may fail as a result one or more of the failure mechanisms in

Table 1.^a In effect, this implies that, given a set of binary inputs, the IC can generate virtually any set of binary outputs.

Table 1. Digital IC failure mechanisms and modes^a

Digital Component	Failure Mechanisms	Failure Modes
CPU (microprocessor) integrated circuits	<ul style="list-style-type: none"> • Die attachment failure • Metallization failure • Contamination • Cracked/fractured • Oxide defects 	<ul style="list-style-type: none"> • High leakage current • Output stuck low • Shorted
Memory (MOS integrated circuit)	<ul style="list-style-type: none"> • Mechanical failure 	<ul style="list-style-type: none"> • Data bit loss • Short • Open • Slow transfer of data
Digital integrated circuit (general)	<ul style="list-style-type: none"> • Contamination • Oxide defects • Wire bond failure • Metallization failure • Die attachment failure • Package-related failure 	<ul style="list-style-type: none"> • Open • Shorted • Output stuck high • Output stuck low • Supply open

^aSource: Adapted from W. Dunn, *Practical Design of Safety-Critical Computer Systems*, Reliability Press, 2002.

Memory and Central Processing Units (CPUs)

From the point of view of safety-critical design, a worst-case failure mode should be assumed for memory systems,⁸ in which the memory, when given an input address, could fail to return requested stored data or instruction or both, or fail to store data. Failing to store data correctly (memory “write” failure) may not have an immediate effect, but a problem could obviously occur when an incorrect datum is read. The situation could be even more complex if the memory failure results in the CPU reading an incorrect instruction. The result could be that the CPU would be running a random program, with data being interpreted as instruction and vice versa. More than likely, the result will be that the CPU will run in a loop or come to a halt. If the CPU is involved in a safety function, the result could be disastrous unless this failure mode is detectable.

CPU functional failure modes are similar to memory when seen from a worst-case failure mode point of view — the failed CPU may output incorrect data or “crash” (come to a halt), which could result in an unsafe situation. Table 2 shows the effect of failure of the various CPU components.⁸

^aSilicon bulk defects, not shown in Table 1, are also a known failure mechanism that may cause the chip to fail to perform its intended I/O function.

Data Communication Link

The computer system may communicate with the outside world through a data communication link (Figure 1). Failures in the communication link actually reduce to (1) failure to receive or transmit data, and (2) corruption of received or transmitted data.

Table 2. Functional failure modes of the CPU^a

Failed Central Processing Unit Components	Local Effect of the Failure
ALU	Arithmetic or logical operation yields incorrect results.
Instruction decoder and pointer	Generates incorrect address causing memory to return incorrect contents.
Accumulator(s) and registers(s)	Potential alteration of correct data or address.
Input port	Alters correct input data
Output port	Alters correct output data.
Memory data interface.	Alters data written to memory or data and instructions read from memory.
Memory address interface.	Alters correct address before memory addressing.

^aSource: Adapted from W. Dunn, *Practical Design of Safety-Critical Computer Systems*, Reliability Press, 2002.

2.2.3. Software Failures

Software consists of instructions and data residing in the hardware. The instructions will function correctly and in the same way for as long as the hardware is functioning correctly. Simple software can be written to be error free. Everyday examples of this include the software in automotive systems, the microwave oven, the video cassette recorder (VCR) and the digital video disc (DVD) player. The problem comes when the requirements become sufficiently complex. In general, software faults can originate from the following sources:

- a) application software (software generated by the designer);
- b) system software (used to host the application software in real time and to provide an interface between it and the application software);
- c) development software (software that is typically used to compile the application source code into runtime code).

In general, software faults will have the same effect as hardware failures in CPU or memory.⁸ Significant faults in the software may cause the program to crash and/or to set or reset some output bits that it are not supposed to set or reset.

The literature on software failures^{9, 10, 11} identifies two main interpretations of the concept of software failure. One interpretation views “failure” as a property of the software itself. That is, the software is considered in isolation and not as a part of the hardware in which it resides. Another view sees the concept of software failure as meaningless unless it is viewed as an integral part of the hardware in which it resides.¹² Chu et al.¹² identify six stages of the software development life cycle (SDLC) as (1) system engineering and modeling, (2) software requirements analysis, (3) software analysis and design, (4) code generation, (5) testing, and (6) operation and maintenance. An error can be introduced at any stage of the SDLC. The testing stage attempts to discover these errors with the objective of fixing them. However, especially for complex systems, it is difficult to discover all errors. In practice one has to assume that an undiscovered error remains (especially for complex systems, this is in fact often the case) when the system becomes operational.^a Typically, a system may function normally for quite some time until, when the right set of conditions occur, such an error (dormant error) may be discovered (i.e., becomes active). Thus, a software failure occurs as a result of the combination of a dormant error and the onset of the specific set of conditions that triggers the error. In general, it is difficult to predict the impact of a triggered fault. The fault may cause the system to behave in undesirable ways. In addition, since the fault is unknown, it is difficult to predict how it will impact the system when it does occur.

2.2.4. Systematic Faults

Systematic faults include the following:

- environmental conditions such as temperature, humidity, radiation, vibration, and EMI/RFI;
- human errors, including errors introduced during manufacturing and/or programming, installation, testing, and maintenance; and
- design faults, introduced during hardware or software design.

^aWhile developing the avionics software for the space shuttle, NASA determined that the statistical average for software used in critical systems (e.g., flight control, air traffic control, etc.) averaged 10 to 12 errors for every 1000 lines of software code. Because this was unacceptable to NASA for use on the space shuttle, NASA forced one of the most stringent test and verification processes ever undertaken for the primary avionics system software. An analysis performed after the Challenger accident showed that the primary avionics system software (PASS) for the space shuttle had a latent defect rate of just 0.11 errors per 1000 lines of code. However, this achievement did not come easily or cheaply. In an industry where the average line of code costs the government (at the time of the report) about \$50 (written, documented, and tested), PASS cost NASA slightly over \$1000 per line. The total cost for the initial development and support for PASS was \$500 million.

3. DIGITAL I&C FAILURES IN THE PETROCHEMICAL INDUSTRY

3.1. Offshore Reliability Data

Several web searches were performed to identify failure information for digital equipment used in the petrochemical industry. One source of information located is the *Offshore Reliability Data* (OREDA, www.oreda.com), a database project sponsored by nine oil and gas companies with worldwide operations. It contains information on equipment performance during normal operation. Basically, the following type of information is collected:

- equipment and operational characteristics (one record for each equipment unit);
- failure data (one record for each failure); and
- maintenance data (one record for each maintenance task, both corrective and preventive maintenance).

While only participating companies can get direct access to the OREDA database, the organization also publishes the data in generic form in reliability handbooks. The handbooks provide both quantitative and qualitative information as a basis for “reliability, availability, maintenance and safety (RAMS)” analyses.

Four handbooks have been issued since 1984, the last edition (no. 4) in October 2002. The fourth edition was used in this study. Reliability data are provided on classes and subclasses of equipment, as shown in Table 3.

Table 3. Classes and subclasses of equipment for which reliability data is provided in OREDA

- | | |
|---|--|
| <ul style="list-style-type: none">• MACHINERY<ul style="list-style-type: none">○ Compressors○ Gas turbines○ Combustion engines○ Turboexpanders
• ELECTRIC EQUIPMENT<ul style="list-style-type: none">○ Electric generators○ Electric motors
• MECHANICAL EQUIPMENT<ul style="list-style-type: none">○ Heat exchangers○ Vessels○ Heaters and boilers | <ul style="list-style-type: none">• CONTROL AND SAFETY EQUIPMENT<ul style="list-style-type: none">○ Fire and gas detectors○ Process sensors○ Valves
• SUBSEA EQUIPMENT<ul style="list-style-type: none">○ Control systems○ Manifold○ Flowline○ Subsea isolation system○ Risers○ Running tool○ Wellhead and X-mas tree |
|---|--|

3.1.1. Control and Safety Equipment Category

As can be deduced from Sect. 3.1, most of the equipment failure data in the OREDA handbook deals with mechanical and electro-mechanical equipment. Since the focus of this study is on digital I&C equipment, only the “Control and Safety Equipment” category as well as the control systems in the “Subsea Equipment” category were selected for further review. The “Control and Safety Equipment” category

includes fire and gas detectors, process sensors, and valves. The boundary definition^a for a fire or gas detector is shown in Figure 2. This subcategory was included in our review because the address/interface unit was assumed to include digital components.

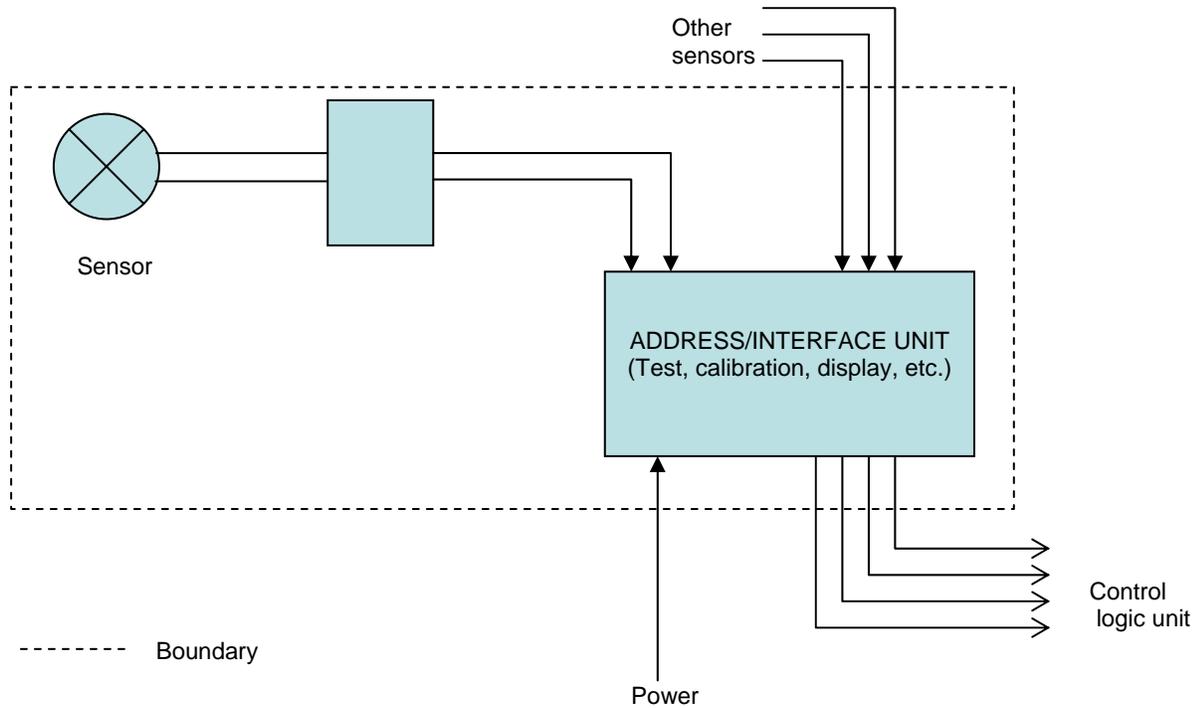


Figure 2. OREDA boundary definition for fire and gas detectors

The failure modes, number of failures, and mean failure rates as documented in OREDA 2002 are shown in Table 4.

3.1.2. Control Systems in Subsea Equipment Category

The boundary definition for control systems in the subsea equipment category is shown in Figure 3. It applies to subsea production/injection control systems, controlling single satellite wells and more complex subsea production facilities such as multi-well manifold template systems. As in the case of Figure 2, the controls systems in the subsea category was included in our review under the assumption that some of the control subsystems contain digital I&C modules, as do many I&C systems of this nature. The failure rates are shown in Table 5.

^aThe boundary definition identifies an area, and all the components within it are regarded as being part of one system or subsystem for the purposes of failure identification and analysis.

Table 4. Failure modes failure rates of fire and gas detectors with embedded digital electronics

Failure mode	No. of failures	Mean failure rate (10⁶ hours)
ITEM: Fire and Gas Detectors (Control and Safety Equipment Category)		
Aggregated operational time in service (10 ⁶ hours).....26.9668		
Population:..... 858		
CRITICAL (total)	47	1.10
Fail to function on demand	12	0.21
No output	5	0.3
Spurious high-level alarm signal	9	0.18
Spurious low-level alarm signal	5	0.14
Spurious operation	16	0.38
DEGRADED (total)	232	9.44
Erratic output	44	1.43
Fail to function on demand	6	0.22
High output	10	0.38
High output, unknown reading	22	0.34
Low output	4	0.17
Low output, unknown reading	1	0.09
Minor in-service problems	5	0.14
Other	23	1.25
Spurious low-level alarm signal	1	0.03
Unknown	4	0.13
Very low output	112	5.43
INCIPIENT		
Minor in-service problems	76	4.33
UNKNOWN	8	0.31

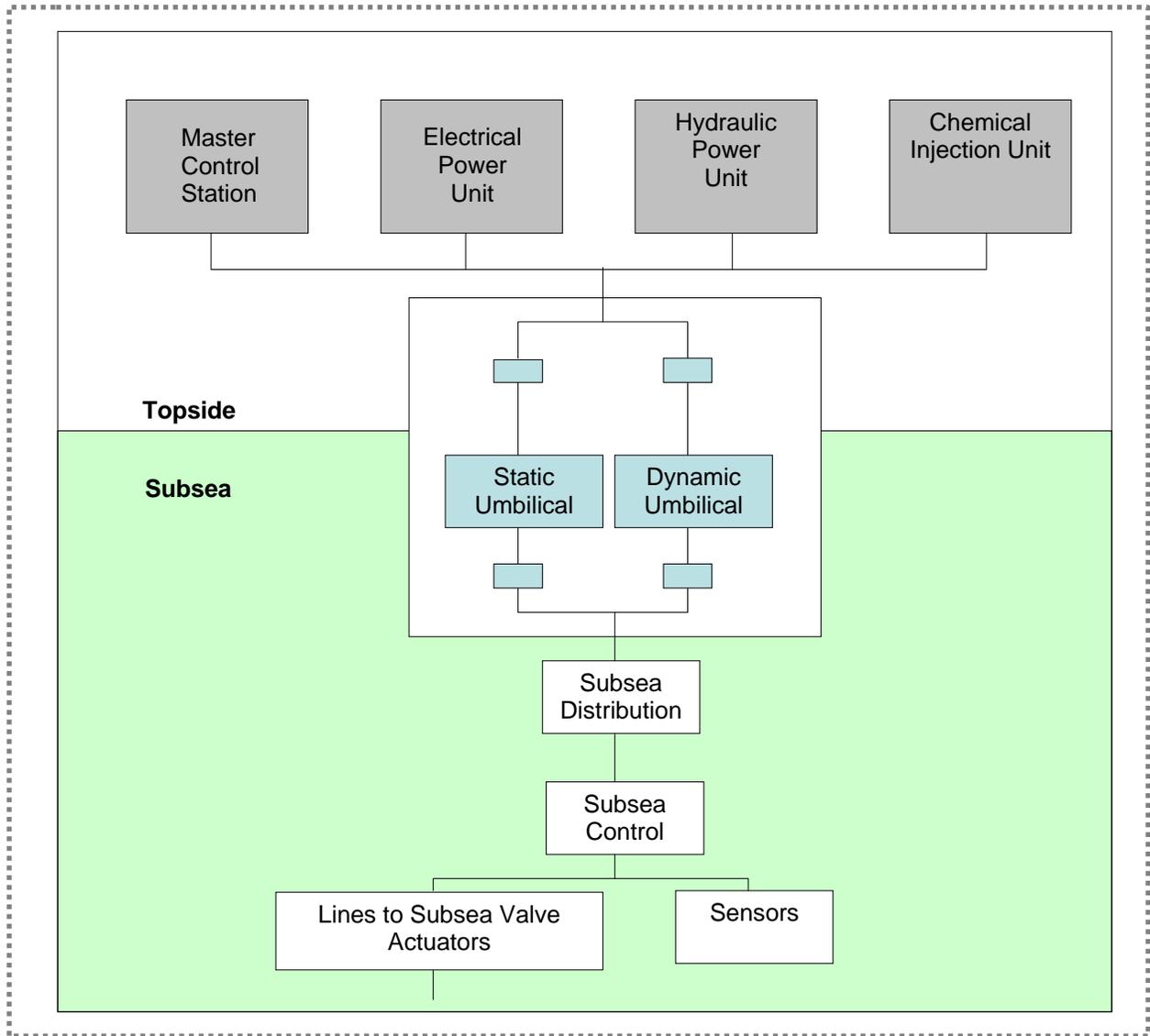


Figure 3. OREDA boundary definition for control systems within the subsea equipment category

Table 5. Component failure rates of control systems in subsea equipment

Component	Mean failure rate (10⁶ hours)
ITEM: subsea production/injection control systems Aggregated operational time in service (10 ⁶ hours)... = 0.8531	
Chemical injection unit (topside)	0.4854
Electrical power unit (topside)	119261
Hydraulic power unit (topside)	13.8661
Master control station (topside)	59.3623
Dynamic umbilical (includes hydraulic/chemical line, power/signal line, sheath/armor/subsea umbilical, termination unit, topside umbilical, and termination unit)	4.2669
Static umbilical (includes hydraulic/chemical line, power/signal line, sheath/armor/subsea umbilical, termination unit, topside umbilical, and termination unit)	
Sensors (includes pressure, temperature, flow, sand detection, and valve position sensors)	9.1973
Subsea control module	49.5976
Subsea distribution module	35.4531

4. DIGITAL I&C FAILURES IN THE AVIATION INDUSTRY

4.1. Introduction

Modern aircraft contain a great degree of automation. In fact, the term “fly-by-wire” has become a public “buzzword” for computers in the cockpit, although it refers technically to the replacement of the physical link to the flight controls with a digital link (i.e., computer control). All aircraft designed and built within the last 15 years have some computer technology in the cockpit, and they are reported to have a better safety record than older aircraft.¹³ However, it is unclear how much of this increased safety record is due to the use of digital technology/computers. We reviewed the literature as well as aviation databases in an attempt to gain some insights in the use of digital technology and how that might impact the nuclear power plant (NPP) environment.

4.2. The Aviation Safety Information Analysis and Sharing (ASIAS) System

The Aviation Safety Information Analysis and Sharing (ASIAS) System was located through several web searches and contacts with cognizant personnel¹⁴ at the Federal Aviation Administration (FAA). The ASIAS system is a facility for the integration, analysis, and sharing of aviation safety data and information. Information at the ASIAS website describes the system as one that “enables users to perform integrated queries across multiple databases, search an extensive warehouse of safety data, and display pertinent elements in an array of useful formats.” The Accident/Incident Data System (AIDS) database¹⁵ contains data records for general aviation and commercial air carrier incidents since 1978. The ASIAS database for AIDS contains incidents only because ASIAS uses the National Transportation Safety Board (NTSB) accident database as the primary source for accident information.

The AIDS database was searched for digital-instrumentation-related incidents. Keywords that were successful in identifying digital/computer-related incidents were *Computer(s)*, *Instrument(s)*, *Digital*, *Instrumentation*, and *Control*. The total number of reports in the database was 86,682. Out of this, 67 incidents were identified as computer-related. From the narratives provided for those incidents, the listed causes of failure were further divided into subcategories:

- **False Indication:** Erratic behavior of some subsystem, which cleared when a computer was replaced.
- **Failed Execution:** Clear indication in the narrative that computer failed to execute its function.
- **Calibration Problems:** The errors were due to calibration problems of some kind.
- **General Computer-Related Problems:** The malfunction was traced to a computer failing to function properly, but another component also had to be replaced.
- **Physical Failure:** Clear indication in the narrative that computer completely “died.”
- **General Instrument Problems:** Digital instrumentation problems.
- **Accessory Failure:** A failure, not directly related to a computer or other digital instrument, but that resulted in the computer not working. An example is a circuit breaker failure.

The subcategories and the number of failures in each subcategory are shown in Table 6. The percentage of overall failures that each subcategory represents is shown in Figure 4. Computer failures from 1980 to present over 5-year time periods were investigated in an attempt to make conclusions regarding

Table 6. Computer-related failure subcategories

Subcategory	Abbreviation used In chart	Explanation of subcategory	Number of incidents in subcategory						
			1979 and Prior 9955*	1980 – 1985 20,701*	1986 – 1990 18,703*	1991 – 1995 15,266*	1996 – 2000 11,870*	2001 – Present 10,187*	TOT 86,682*
False indication	FLS_IND	Erratic behavior of some subsystem, which cleared when a computer was replaced.	1	4	1	3	2	0	11
Failed execution	FLD_EXEC	Clear indication in the narrative that a computer failed to execute its function.	1	5	0	1	0	1	8
Calibration problems	CAL_PRB	The errors were due to calibration problems of some kind.	0	4	4	1	1	0	10
General computer-related problems	GEN_COMP	The malfunction was traced to a computer malfunction/failure but at least one other component also had to be replaced.	0	1	5	5	5	2	18
Physical failure	PHY_FLR	Clear indication in the narrative that a computer completely “died.”	0	0	4	2	3	3	12
General instrument problem	GEN_INST	Digital instrumentation problems.	0	0	1	1	1	1	4
Accessory failure	ACC_FLR	A failure, not directly related to the failure of a computer or other digital instrument, but that resulted in the computer not working. An example is a circuit breaker failure or an antenna failure.	0	0	1	0	1	2	4

improvements in reliability of aviation computers. The number of failures in each of the five-year periods is also shown in Table 6. While the actual number of failures in the five-year periods is not many, there appears to be a general trend toward fewer failures over the years. In the FLD_EXEC^a category for example, in which the records in the database indicate that a computer is the sole source of the malfunction, there is an 80% reduction in the number of failures from 1980 to present. (Note that the database was started in 1978, so the column containing data “1979 and Prior” represents only little more than a year of information).

A computer failure rate for the commercial aviation industry was estimated using this data. It should be noted that this is only a rough estimate based on data we were able to assemble in the relatively short period of this study. The primary assumption that the number of incidents reported (67) is representative of the industry is probably a nonconservative assumption. That is, it is likely that most of the incidents that occurred were not reported because the reporting system is voluntary. Understanding this, the objective of this estimate is to get a “feel” for what a lower-bound estimate of the failure rate might be in a power plant environment (at least within an order of magnitude). This will be informative for nuclear I&C regulation, the rationale being that since the qualification process for nuclear I&C safety systems is arguably the most stringent compared to other industries, such as aviation, digital I&C in nuclear power plants is likely to be acceptably reliable if the same is proven for the aviation industry.

The estimated failure rate λ is given by:

$$\lambda = \frac{N}{T} \tag{1}$$

where

N is the number of computer failures reported, and
T is the aggregated time in service.

Based on the number of revenue hours that aircraft were available for domestic and international flights from 1980 to 2004 and the number of aircraft (Table 7)^b, the aggregated time in service was estimated to be $\sim 3.36 \times 10^8$ h. This corresponds to an availability of almost 30%. The failure rate is then

$$\lambda = \frac{67}{3.36 \times 10^8 h} = 2.00 \times 10^{-7} / h \tag{2}$$

Again, because the reporting system is voluntary, the number of incidents occurring is likely to be greater than the 67 identified, and the $2.00 \times 10^{-7}/h$ would be a lower-bound estimate.

This result will be referred to in our discussion on digital I&C failures in domestic nuclear power plants (Chapter 6).

^aEach of the abbreviations used to identify a failure type is defined in Table 6.

^bhttp://www.bts.gov/publications/national_transportation_statistics/html/table_air_carrier_profile.html

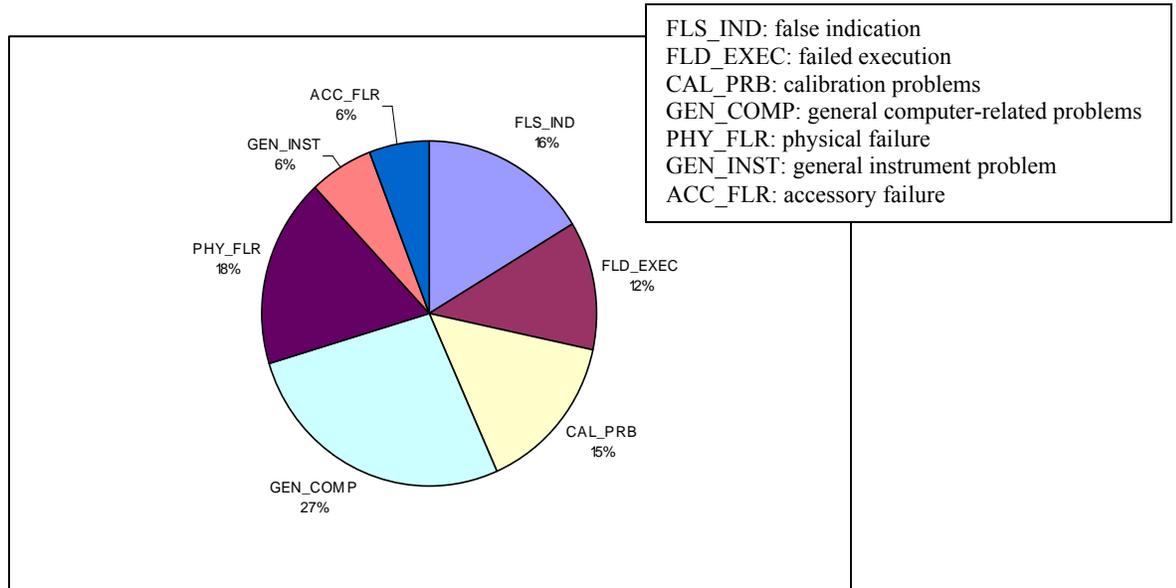


Figure 4. Computer-related failures in each subcategory from 1978 through 2006

Table 7 Availability of commercial aircraft

(Source: U.S. Bureau of Transportation Statistics,

http://www.bts.gov/publications/national_transportation_statistics/html/table_air_carrier_profile.html)

Calendar year ^a	Domestic revenue hours	International revenue hours	Total revenue hours	Number aircraft available for service	Availability of aircraft (%)
1980	6,247,795	819,518	7,067,313	2818	29
1990	9,717,375	1,566,760	11,284,135	4727	27
1994	10,721,374	1,978,381	12,699,755	5221	28
1995	11,378,134	2,021,060	13,399,194	5567	27
1996	11,871,886	2,113,467	13,985,353	5961	27
1997	12,060,253	2,235,441	14,295,694	5770	28
1998	12,445,483	2,394,095	14,839,578	6114	28
1999	13,091,273	2,456,726	15,547,999	6254	28
2000	13,905,472	2,595,893	16,501,365	6522	29
2001	13,507,906	2,569,314	16,077,220	6081	30
2002	13,727,415	2,495,108	16,222,523	5819	32
2003	15,245,620	2,593,690	17,839,580	6675	31
2004	16,223,363	2,841,354	19,064,717	Unavailable	~33
Total	169,039,410	30,267,138	199,306,548		28

^aData not reported for all years.

5. FAILURES IN THE PUBLIC TELEPHONE NETWORK

5.1. Reasons for Investigating Failures in the Telephone Network

Although the public telephone network is not typically considered as a failure-critical system, this system was nevertheless investigated for sources of failures for several reasons: For one thing, telephone switch manufacturers are among the world's leaders in computing technology.^{16,17} They dedicate a significant amount of research on developing highly reliable systems, and their software development processes typically incorporate the most sophisticated practices, supplemented by elaborate quality assurance functions. Like most large distributed systems, the U.S. public switched telephone network (PSTN, perhaps the largest distributed system in the world) depends on software, hardware, and human operators and maintainers to function correctly. Although the basic task of the PSTN is simple — it connects point A with point B — this task requires some of the most complex and sophisticated computing systems in existence. For example, software for a switch with even a relatively small set of features may comprise several million lines of code.¹⁶ Since the PSTN contains thousands of switches, the software complexity can be very significant.

For these reasons, it was felt that a review of failure sources in the telephone switch system might enable some conclusions to be drawn with regard to software reliability in a failure-critical environment such as a nuclear power plant.

5.2. Results of Literature Review

Kuhn¹⁶ analyzed sources of failure in the U.S. PSTN over a two-year period (1992 to 1994). Table 8 shows failure effects, by categories and sources, for outages^a from April 1992 to March 1994. The fifth column, "Customer Minutes," is the number of customers affected multiplied by the outage duration in minutes. Customer minutes are a more realistic measure of a disruption's magnitude as a basis for comparing failure data than outage duration alone.^{16, b} In the human-error category, Kuhn separated errors by telephone company personnel from those made by nonemployees only because "the companies have direct control over employees only." Overload conditions are accounted for separately because "they represent failures accepted as an engineering trade-off between dependability and cost." The percentage of outages attributed to each of the major categories in Table 8 is shown in Figure 5. Figure 6 shows the downtime in customer minutes by category. Kuhn's results show that the number of failures in each failure category, and the effect of the failure, differ significantly for most failure categories. For example, overloads caused only 6% of the total outages; however, they account for nearly 50% of the total customer minutes. Customer minutes, rather than outage duration alone, are a more realistic measure of the magnitude of a disruption as a basis for comparing failure data.¹⁶ Human error caused nearly 50% of the outages, but only little more than a quarter of the downtime. One interesting finding — given the complexity of the PSTN, its significant reliance on software, and potential lessons learned for the nuclear power plant environment — was that software errors caused less system downtime (2%) than any other source of failure except vandalism. The effect of hardware and software failures were similar in terms of average number of customers affected (96,000 and 118,000) and duration of outage (160 and 119 minutes, respectively).

^aTelephone companies are required to notify the FCC of outages affecting more 30,000 customers. These outage records were used by Kuhn to determine the principal causes PSTN failures.

^bFor example, a 20-minute outage affecting 10,000 customers (200,000 customer minutes) is considered more severe than a 30-minute outage affecting 1000 customers (30,000 customer minutes).

Table 8. Failure effects by categories and sources, for outages from April 1992 to March 1994^a

Categories and sources	No. of outages	Average no. of customers affected	Average outage duration (minutes)	Customer minutes (in millions)
Human error – company	77	182,060	149.4	2,349.3
Cable maintenance	8	66,900	168.9	61.3
Power supply maintenance	19	292,980	150.4	879.1
Power monitoring	4	71,000	185.2	36.5
Facility or hardware board maintenance	15	169,370	134.7	242.7
Software versions (mismatches)	13	127,020	176.5	189.2
Following software maintenance or upgrade	8	225,960	204.2	871.2
Data entry	10	163,300	60.6	69.3
Human errors – others	73	83,936	360.1	2,415.8
Cable cuttings	64	78,690	355.6	1852.5
Accident	9	121,240	392.0	563.3
Acts of nature	32	159,000	828.2	3,124.0
Cable	13	13,000	717.6	784.8
Power supply	7	201,000	236.0	532.5
Facility	10	111,820	1,064.7	312.9
Natural disaster	2	1,200,000	2,437.0	1,493.8
Hardware failures	56	95,690	159.8	1,210.8
Cable component	2	125,000	46.0	5.7
Power supplies	14	112,000	103.9	369.9
Facility component	34	80,840	201.6	748.1
Clock or clock synchronization	6	130,670	91.0	87.1
Software failures	44	118,200	119.3	355.5
Normal operation	13	93,020	187.5	102.6
Recovery mode	31	124,940	86.8	252.9
Overloads	18	276,760	1,123.7	7,527.2
Vandalism	3	85,930	456.0	110.5

^aSource: D. R. Kuhn, *IEEE Computer*, 30(4), April 1997.

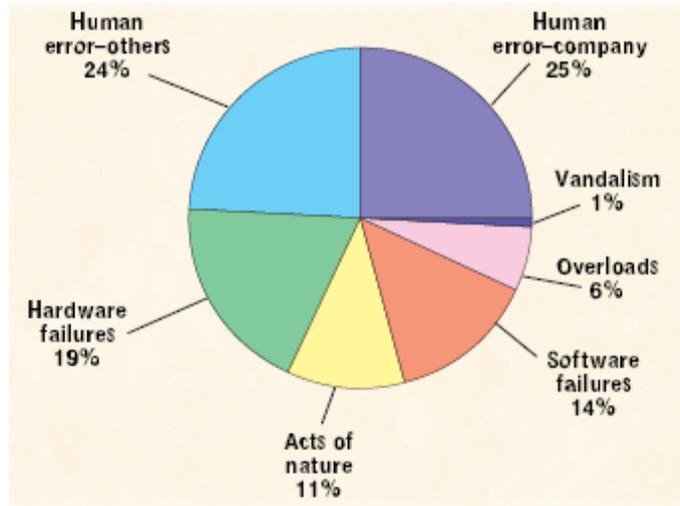


Figure 5. Number of telephone outages by category
 (source: D. R. Kuhn, *IEEE Computer*, 30(4), April 1997)

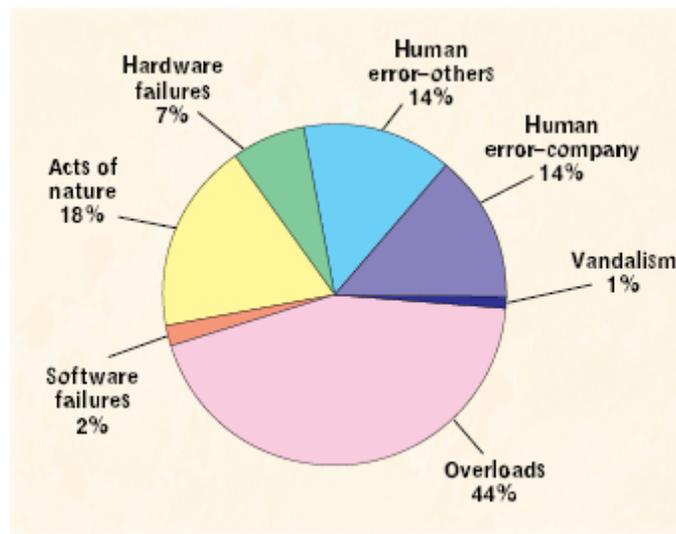


Figure 6. Downtime as measured in customer minutes, by category
 (source: D. R. Kuhn, *IEEE Computer*, 30(4), April 1997)

6. DIGITAL I&C FAILURES IN DOMESTIC NUCLEAR POWER PLANTS

6.1. Introduction

The goal of this study was to survey the nuclear and nonnuclear industries for available sources of digital I&C failures in failure-critical applications. For the NPP studies, LERs and other NRC-related databases were not to be used for this survey. In addition, INPO's EPIX database was not surveyed for I&C failures.

This section briefly reviews failure data used in PRAs for Generation III (Gen III)^a plants. Gen III plants were selected for this review because the PRAs for these plants are expected to use the most recent, up-to-date failure data.

Although copies of the databases for component failures may be proprietary, expensive, or difficult to obtain, the actual data are available through the PRA reports. For example, the IAEA compiled component reliability data from publicly available literature. The IAEA database consists of ~1000 records on 420 component types compiled from 21 different data sources and includes data for nuclear power plant components typically modeled in PSAs.¹⁸ The failure rates for instrumentation given in the IAEA database are primarily from the following documents:

- *Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants*, NUREG/CR-1740, 1984.
- *Interim Reliability Evaluation Program Procedures Guide*, NUREG/CR-2728, January 1983.

Because these are NRC reports, the types of I&C components, their failure rates, and their failure modes were not evaluated.

6.2. Some Failure Rate Information for Gen III Plants

6.2.1. Lungmen, a GE ABWR

Lungmen Units 1 and 2 are GE ABWRs located in Taiwan. Because both units are under construction and should be operational around 2009 and 2010, any data used in the PRA should be more current and up-to-date than any operating nuclear power plant. The ABWR PRA was completed in 1996. The primary values recommended by GE for component failure rates are in

- *General Electric Failure Rate Data Manual*, NEDE 22056, Rev. 2, 1986 (Proprietary).

The principal data sources for the instrumentation failure data used in the Lungmen PRA (from Appendix AA in the *Preliminary Safety Analysis Report for Lungmen Units 1 & 2*) are

^aGen III reactor is a development of any of the generation II designs incorporating evolutionary improvements in design which have been developed during the lifetime of the Gen II designs, such as improved in fuel technology, passive safety systems, and standardized design. Examples of Gen III designs are the Advanced Boiling Water Reactor (ABWR), which first went on line in Japan in 1996, and the European Pressurized Reactor (EPR). Gen III+ reactors are advanced designs that are part revolutionary but fall short of the Gen IV prototypes by being at least part evolutionary. Prototypical of these are the Economic Simplified Boiling Water Reactor (ESBWR) and the AP1000.

- Yen Liao Analysis Annex A, *Component Failure Data* (no date given),
- study done by Barry Simon (GE), Reference NUMAC Field Data (no date given), and
- *Joint Study Report of SSLC Reliability Analysis*, No. IIF-R-389, pp. 7-77 and MIL-HDBK-217C.

One GE study provides the failure rates of digital trip modules and multiplexers. The probability of failure used for the digital trip modules is typically 1.2×10^{-4} , while that of the multiplexers is 1.66×10^{-3} , 3.22×10^{-3} , and 2.40×10^{-4} . Yen Liao's analysis is the basis for the failure rates for the system logic units; the probability of failure used for the system logic units is typically 1.2×10^{-4} .

6.2.2. GE ESBWR

Rev. 1 of the GE ESBWR PRA (*ESBWR Probabilistic Risk Assessment*, NEDO-33201, Rev. 1, and February 2006) was transmitted to the U.S. NRC on February 8, 2006. The generic database is provided in the ESBWR PRA. The generic reliability data for the ESBWR PRA are primarily based on the following two documents

- *Advanced Light Water Reactor Utility Requirements Document*, Vol. II, ALWR Evolutionary Plant, EPRI, 1990.
- *Advanced Boiling Water Reactor Standard Safety Analysis Report*, GE Nuclear Energy, 23A6100, Rev. 9, Aug. 1996.

Other sources of generic data, used as necessary to supplement the above two documents, include the following:

- NUREG/CR-4550, Vol. 1, *Analysis of Core Damage Frequency: Internal Events Methodology*, Rev. 1, January 1990.
- NUREG-1816, *Independent Verification of the Mitigating Systems Performance Index (MSPI) Results for Pilot Plants*, February 2005.
- IEEE Std. 500, *Reliability Data*, Std. 500-1984, December 1984.
- NUREG/CR-2728, *Interim Reliability Evaluation Program Procedures Guide*, January 1983.
- NUREG/CR-2815, *Probabilistic Safety Analysis Procedure Guide*, Brookhaven National Laboratory, August 1985.
- WASH-1400, *Reactor Safety Study, An Assessment of Accidents in U.S. Commercial Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, October 1975.
- NUREG/CR-1740, *Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at US Commercial Nuclear Power Plants*, 1984.
- *General Electric Failure Rate Data Manual*, NEDE 22056, Rev. 2, 1986 (Proprietary).
- study done by Barry Simon (GE), Reference NUMAC Field Data (no date given).

Failure rates for the microprocessor-based components and discrete logic components vary depending on a mean time between failures (MTBF) of 100k hours ($\lambda = 1.0 \times 10^{-5}/h$) or 200k hours ($\lambda = 5.0 \times 10^{-6}/h$). The probabilities of failure of the solid state components are based on the assumption that 95% of the component failures will be detected by self-testing, performed every 30 min. It is further assumed that the remaining 5% will be detected only during surveillance tests performed quarterly (2190 h). The failure rates and failure probabilities of the solid-state components are given in Table 9.

Table 9. Solid-state component failure rate and failure probabilities used in the GE ESBWR PRA

Solid-state component	Failure probability or failure rate
Trip logic unit (TLU) fails to trip	9.0×10^{-4}
TLU bypass logic card fails to transfer	9.0×10^{-4}
Digital trip module (DTM) (safety system) fails to trip	6.0×10^{-4}
DTM/TLU and multiplexer (MUX) interface unit (nonsafety system) fails to trip	9.0×10^{-4}
Remote multiplexing unit (RMU) fails to operate	$5.0 \times 10^{-6}/h$
Essential multiplexing system (EMS) fails to function	$1.0 \times 10^{-5}/h$
Voting logic card fails	2.8×10^{-5}
1/N logic card fails	3.0×10^{-4}
Electromechanical relay fails to operate	1.0×10^{-4}

6.2.3. AP600 and AP1000

The AP600 and AP1000 are both next-generation Westinghouse-designed PWRs. Both have received their final design approvals (FDAs) from the NRC. Data for the AP600 PRA¹⁹ and the AP1000²⁰ are generally derived from

- *Advanced Light Water Reactor Utility Requirements Document*, Vol. III, ALWR Evolutionary Plant, EPRI, 1990.

When ALWR URD failure data were not available, or deemed not applicable for the AP600 or the AP1000, the data were obtained from the following sources, in the order listed.

- NUREG-2728, *Interim Reliability Evaluation Program Procedures Guide*, January 1983.
- IEEE Std. 500, *Reliability Data*, Std. 500-1984, December 1984.
- NSAC-154, *ISLOCA Evaluation Guidelines*, ERIN Engineering and Research, Inc. (prepared for EPRI), September 1991.
- ENEA/ENEL paper “In Search of Aging Factors,” *International Conference on Nuclear Power Plant Aging, Availability Factor and Reliability Analysis*, San Diego, California, July 1985.
- NUREG/CR-4550, Vol. 1, *Analysis of Core Damage Frequency: Internal Events Methodology*, Rev. 1, January 1990.
- “Nuclear Plant Reliability Data System – Failure vs. Calendar Hours (Cumulative) (from 7/74 to 5/94),” Westinghouse Electric Corporation, Report ID #NPRP04AA, Run Date 01/06/95.
- Institute of Nuclear Power Operations (INPO), “Nuclear Plant Reliability Data System (NPRDS).”

The logic and instrumentation failure data for the AP600 and AP1000 microprocessor-based components are derived from Westinghouse data. The failure rates and failure probabilities of the solid-state components used in the PRA for the AP600 and AP1000 are given in Table 10.

Table 10. Solid-state component failure rate and failure probabilities used in the AP600 and AP1000 PRAs

Solid-state component	Failure probability or failure rate
Solid-state relay – fails to operate	$1.0 \times 10^{-7}/\text{h}$
Solid-state relay – spurious operation	$2.0 \times 10^{-7}/\text{h}$
Solid-state time delay relay – fails to operate	$1.0 \times 10^{-6}/\text{h}$
Solid-state time delay relay – premature operation	$5.0 \times 10^{-7}/\text{h}$
Single logic card – all mode failures	$5.0 \times 10^{-6}/\text{h}$
Logic group processing – failure upon demand	1.16×10^{-3}
Logic group processing – spurious failure	$8.01 \times 10^{-6}/\text{h}$
Logic group I/O – failure of output	2.09×10^{-3}
Output logic group I/O – spurious failure	$8.40 \times 10^{-6}/\text{h}$
Modulating logic group or I/O group – failure	8.74×10^{-4}
Input group – failure	5.02×10^{-3}
Input group – spurious failure	$2.74 \times 10^{-5}/\text{h}$
MUX logic group – failure	6.35×10^{-4}
MUX transmitter to group – failure	8.00×10^{-5}
Signal selector logic group – failure	3.46×10^{-3}
Actuation logic group – failure	4.07×10^{-3}
Actuation logic group – spurious failure	$2.04 \times 10^{-5}/\text{h}$
Output logic group selector – failure	8.00×10^{-5}
Output logic group selector – spurious failure	$1.00 \times 10^{-10}/\text{h}$
S-signal sensor – failure	1.00×10^{-6}

6.2.4. ACR-700

The PSAs for the Canada Deuterium-Uranium (CANDU) and Advanced CANDU Reactor (ACR) plants use a generic CANDU reliability database for the calculation of frequencies and probabilities of component failures. The data are based on the operating experience of CANDU plants and were accessed through system and equipment reliability analysis (SERA) reports and station quarterly technical reports. Where required data were not available, data from other sources such as Ontario Power Generation's

(OPG's) fossil-fuel station operating experience and external sources were used. Data based on fossil-fuel station experience were accessed through thermal outage and maintenance activity system (THOMAS) reports.

To supplement its database where necessary, OPG consulted several other sources of published data available from industry sources. The following were their primary sources.

- IEEE, 1984, *Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*. IEEE Std. 500.
- SRI, 1983, *Nuclear Plant Reliability Data System 1982 Annual Reports of Cumulative System and Component Reliability*, Southwest Research Institute, San Antonio, Texas. Proprietary.

The IEEE standard provides failure rates that correspond to various failure modes of electrical and I&C components, including detailed classification with respect to characteristics such as type and size. However, for some components, the failure rate data are not available for all type or size classifications.

The NPRDS annual report presents data that span eight years of experience with commercially operated U.S. nuclear power plants through 1982. The report provides component failure information such as the total number of failures, the population, total component operating times, and failure modes. Data from published external sources, such as NPRDS, SERA, and IEEE Standard 500-1984, were used only when OPG data were not available.

7. CONCLUSIONS AND RECOMMENDATIONS

This letter report documents the results of a survey of some industry databases, as well as a search of the available literature, to gain some insight into digital I&C failures. The focus of the study was on nonnuclear industries with failure-critical applications. Although the study was to include nuclear I&C failure information that could be obtained within the study period, specific research direction from the NRC excluded the use of LERs and other NRC-related databases.

Based on the data that could be assembled in the relatively short period of this study, computer failure rate in the commercial aviation industry was estimated to be 2.0×10^{-7} /h. However, because the reporting system for the database used (the ASIAs/AIDS database) is voluntary, this value represents a lower bound estimate. Failure rates of "Control and Safety Equipment" for offshore systems were found to range from 3×10^{-8} /h to 1.1×10^{-6} /h. For telephone network systems, one study 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.

This study did not focus specifically on digital I&C failure data from NASA; however, one interesting study result by NASA on software errors was documented in this report. In particular, while developing the avionics software for the space shuttle, NASA determined that the software used in critical systems (e.g., flight control, air traffic control) averaged 10 to 12 errors for every 1000 lines of software code. Because this was unacceptable to NASA for use on the space shuttle, NASA forced one of the most stringent test-and-verification processes ever undertaken for the PASS software. An analysis performed after the Challenger accident showed that the PASS software for the space shuttle had a latent defect rate of just 0.11 errors per 1000 lines of code. However, this achievement did not come easily or cheaply. In an industry where an average line of code costs the government (at the time of the report) about \$50 (written, documented, and tested), PASS cost NASA slightly over \$1000 per line. The total cost for the initial development and support for PASS was \$500 million.

Failure data used in PRAs for Gen III nuclear power plants were briefly reviewed in this study. Gen III plants were selected for this review because the PRAs for these plants are expected to use the most recent, up-to-date failure data. Failure rates for microprocessor-based components and discrete logic components were found to vary between 5×10^{-6} /h and 1.0×10^{-5} /h. The probability of failure on demand for solid-state components was found to range from 2.8×10^{-5} to 9×10^{-4} . The probability of failure of the solid-state components is based on the assumption that 95% of the component failures will be detected by self-testing, performed every 30 min. It is assumed that the remaining 5% will be detected only during surveillance tests performed quarterly (every 2190 h). In both cases, the mean-time-to-repair is 5 hours.

This brief study indicates that digital I&C failure rates used in the safety assessments in the failure-critical nonnuclear industries are lower than for nuclear power plants. It is recommended that a more detailed study be performed to substantiate this or to determine whether the comparisons are appropriate or not.

It is also recommended that this study be expanded to perform a more detailed review of both the nuclear power industry's digital I&C experience and the commercially available databases. With respect to the nuclear power industry, many PRAs cite 25-year old reports for data and supplement that with recent (internal) studies for I&C components. The product of this detailed review would be a list of failure rates by electronic component. This data would be supplemented with failure modes identified from actual operating experience through a review of the digital I&C failure information from the EPIX database. Information from the commercially available databases (i.e., third-party databases) would complete the review. These databases appear to 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.

8. REFERENCES

1. <http://www.eia.doe.gov/cneaf/nuclear/page/analysis/nucenviss2.html>
2. http://nucleartimes.jrc.nl/Doc/Final_Report.pdf
3. <http://gif.inel.gov/roadmap/>
4. K. Korsah et al., *Environmental Testing of an Experimental Digital Safety Channel*, NUREG/CR-6406, September 1996.
5. T. J. Tanaka, S. P. Nowlen and D. J. Anderson, *Circuit Bridging of Components by Smoke*, NUREG/CR-6476, October 1996.
6. T. J. Tanaka and S. P. Nowlen, *Results and Insights on the Impact of Smoke on Digital Instrumentation and Control*, NUREG/CR-6597, January 2001.
7. P. D. Ewing and R. T. Wood, *Comparison of U.S. Military International Electromagnetic Compatibility Guidance*, NUREG/CR-6782, August 2003.
8. William Dunn, *Practical Design of Safety-Critical Computer Systems*, Reliability Press, 2002.
9. C. Garret and G. Apostolakis, "Context in the Risk Assessment of Digital System," *Risk Analysis*, 19, 23 (1999).
10. *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues*, National Academy Press, Washington D.C., 1997.
11. N. G. Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, Reading, Mass., 1995.
12. T. L. Chu et al., "A Review of Software-Induced Failure Experience," *NPIC&HMIT*, 23 – 36, 2006.
13. <http://www.rvs.uni-bielefeld.de/publications/Incidents/DOCS/Research/Rvs/Article/Vara-opinions.html>
14. Charles W. Kilgore, II, Project Manager & Contracting Officer's Technical Representative (COTR); Software & Digital Systems (SDS) Research Project.
15. http://www.asias.faa.gov/portal/page?_pageid=56,86203,56_86223:56_86227:56_96434&_dad=portal&_schema=PORTAL
16. D. R. Kuhn, *IEEE Computer*, 30(4), April 1997.
17. C. Jones, *Applied Software Measurement*, McGraw-Hill, New York, 1991.
18. International Atomic Energy Agency (IAEA), *Component Reliability Data for Use in Probabilistic Safety Assessment*, IAEA-TECDOC-478, Vienna, 1988.
19. Westinghouse, *Simplified Passive Advanced Light Water Reactor Plant Program, AP600 Probabilistic Risk Assessment*, prepared for U.S. Department of Energy, San Francisco Operations Office, DE-AC03-90SF18495, June 26, 1992.
20. Westinghouse Electric Corporation, *API000 Probabilistic Risk Assessment*, APP-GW-GL-022, 2003.