INSTRUMENTATION AND CONTROL SYSTEM FAILURES IN NUCLEAR POWER PLANTS[1]

Robert W. Brill
U. S. Nuclear Regulatory Commission
MS: T10-L1, Washington, D.C. 20555
Phone: (301) 415-6760 Fax: (301) 415-5074
Email: rwb2 @nrc.gov

KEYWORDS: Instrumentation, Control, Digital, License Event Report

ABSTRACT

Examination of the Licensee Event Report (LER) database, by the Office of Nuclear Regulatory Research, provides a snapshot of instrumentation and control (I&C) impact on plant safety. The LER database consists of all reportable events that could affect the safety of Nuclear Power Plants. The LER database study uncovered digital I&C vulnerabilities in nuclear power plants from operational experience. This study considered digital-related LERs for a five-year period, starting in 1994. The LER study places LERs in three categories: hardware, software, and human/system interface (HSI). Analysis showed an nearly equal distribution of events in each of the three categories. The analysis also showed that approximately 8% of all LERs, from 1994 to 1999, contain digital I&C failures, and 9% of reactor trips for those years are attributed to digital I&C failures. Detailed examination of the digital I&C failures emphasizes that a significant percentage of the failures occurs as a result of failures in the requirements and Verification and Validation life-cycle stages. This database study shows I&C systems, including digital I&C systems, have a noticeable impact on nuclear power plant safety.

INTRODUCTION

Instrumentation and control (I&C) systems are vital to nuclear power plant operation and safety. I&C systems provide operators with important plant information, and they send commands to plant systems. With the introduction of digital technology, I&C systems are now embedded in plant components such as transformers, valves, motor control centers, and circuit breakers. As the U.S. Nuclear Regulatory Commission moves toward a risk-informed, performance-based regulatory environment, a major question arises:

- What is the impact of digital technology on nuclear power plant safety?

The review of the Licensee Event Report (LER) database was instituted to find answers to this question. This study, provides some insight into the vulnerability of digital I&C systems and results of the LER study will help guide future research and regulatory developments regarding digital I&C systems.

NOMENCLATURE

I&C	Instrumentation and Control
LER	Licensee Event Report
V&V	Verification & Validation

LER DATABASE STUDY

The LER database consists of reports from the licensees for types of reactor events and problems that are believed to be significant and useful to the NRC in its effort to identify and resolve threats to public safety. It is designed to provide the information necessary for engineering studies of operational anomalies and trends and patterns analysis of operational occurrences. This database is stored in the Sequence Coding and Search System web site[1].

A study of these LERs was undertaken to determine whether there was sufficient operational experience that could be used to uncover digital I&C system vulnerabilities in nuclear power plants. This examination covered all LERs during the years 1994-1998 and included both digital failures and external events causing digital I&C systems to malfunction. An example of an external event affecting a digital I&C system is a case in which the control room operators received annunciations indicating that nonessential loads from the 600-volt bus had been de-energized. This event was caused by an arcing ground on a freight elevator brake solenoid, which resulted in a trip of the nonessential load lockout logic on the 600-volt bus. The ground also caused a trip of the RPS motor-generator feeder breaker. (The affected breaker

[1] The views expressed in this paper are those of the authors and should not be construed to reflect the U. S. Nuclear Regulatory Commission position.

is equipped with a microprocessor-based trip unit.) The ground affected the trip unit such that its microprocessor actuated the breaker, which in turn tripped the reactor.

The initial analysis placed the selected LERs in three categories: hardware, software, and human/system interface (HSI). (A significant number of the LERs include human errors that did not result in inappropriate operator actions. These are included in the category HSI.) In a number of LERs, the reported problem fell into multiple categories. For example, in one LER, a sudden trip of the main turbine generator resulted in a reactor trip. The reason for the turbine trip included:

- a hardware failure in a digital feedwater control card,
- a software error in the main turbine trip logic allowing a single failure to trip the turbine, and
- an HSI error in which the redundant turbine trip relays were connected in parallel rather than in series.

1.1 LER Analysis Summary

There were 6681 LERS between 1994 -1998, with 385 of those LERs involving digital anomalies. Figure 1 shows the percentage of LERs involving digital anomalies on a per year basis. With the exception of 1994, the number of digital LERs is relatively constant. A possible explanation of the high number of digital-related LERs in 1994 is that it was a year in which utilities performed a number of digital upgrades and startup and learning problems occurred.

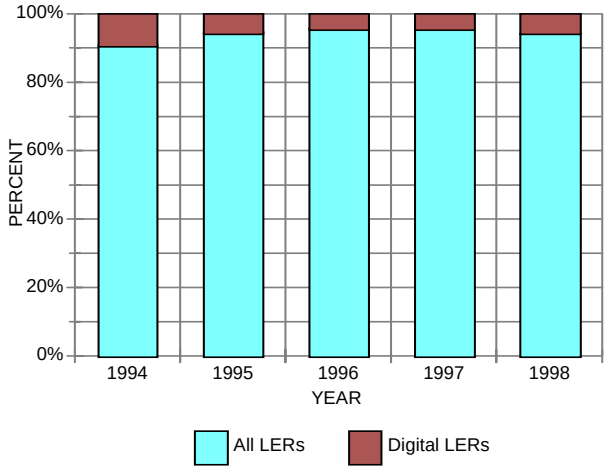

Figure 1. LER Percentages.

There were 484 reactor trips from 1994 - 1998, with digital anomalies contributing to 60 of these. As shown in Figure 2, the percentage of all trips caused by digital anomalies is relatively constant over the time period. Approximately 13% of all digital-related LERs involved a reactor trip.

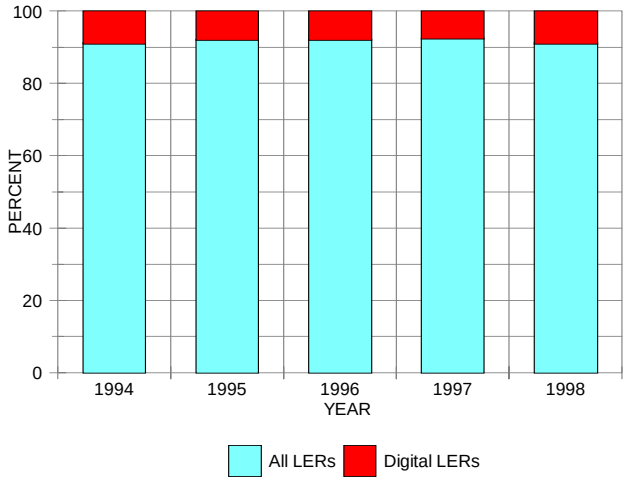

Figure 2. Trip percentages.

The number of digital LERs per category (hardware, software, and HSI) is almost evenly distributed, as shown in Figure 3. A number of the 385 digital events fit into more than one category. For example, there may have been both an HSI failure and a software failure reported in a single LER. Thus the allocation of failures to more than one category accounts for the sum of each type of failure to be greater than the total number of digital failures found in the LERs.

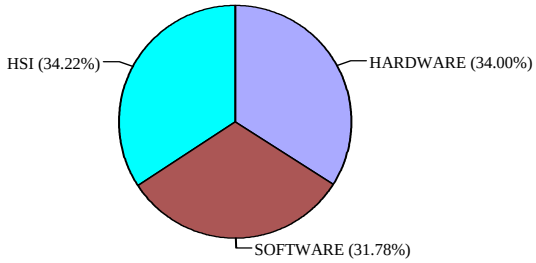

Figure 3. Digital Anomaly Categories

Figure 4 presents the analysis by system type. Digital anomalies in three safety/risk-significant systems (reactor protection, feedwater, and reactor coolant system) contributed to nearly 29% of the LERs. The largest single contributor to the LERs was the plant computer at 28%.

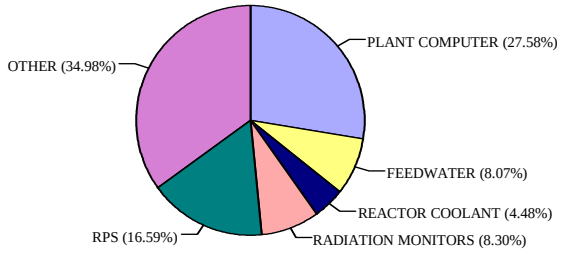

Figure 4. Digital LERS by System

Examination of the hardware LERs shows the distribution of 153 digital hardware failures. This distribution resembles that which would normally occur in an analog system. Figure 5 shows this distribution.

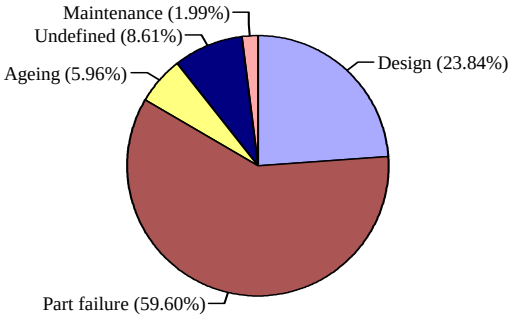

Figure 5. Digital Hardware Failures

Figure 6 presents the analysis of the 143 software events which were found in the LER's. For the analysis, the following definitions were used:

- Requirements error is an inherent error in the procedures, technical specifications, etc. that is replicated in the software.
- Software incomplete is an error that, if software had been designed correctly, with appropriate diagnostics, would not have occurred, this is an error in the requirements.
- V&V error is an error that would have been detected if the requirements, procedures, and software program had been checked properly.
- Software development is an error that occurred because software was written incorrectly by the programmer.
- Logic error is the case when the logic written into code was incorrectly.
- Undefined means there was insufficient information to categorize the source of the problem, and Miscellaneous includes data input errors where personnel input incorrect data. Software could have been written to detect problem but didn't, this is a improper analysis of the requirements.

As can be seen in the figure, the largest category is requirements errors, followed by software being incomplete, which is a form of requirements error. Together the two categories contribute over 53% of the software errors found in LERs.

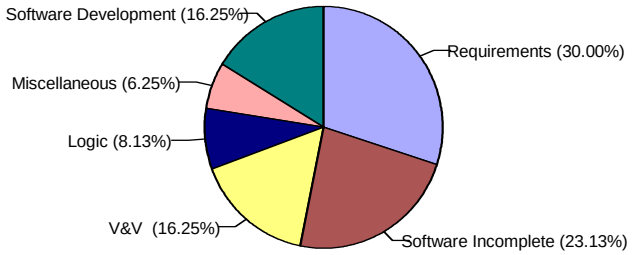

Figure 6. Software Errors

Figure 7 is an analysis of the digital LERs pertaining to human system interface. As can be seen in the figure, for the 154 incidents, approximately 58% of the total consists of problems can be attributed to problems in the requirements. Problems that in the requirements category include: analysis errors, technical specification problems, and procedure errors. The root cause of these is generally caused by inconsistent, ambiguous, and incomplete requirements. The second largest category are maintenance (maintenance and data entry errors) problems. This category contributes 26% of the total. The following definitions were used for this analysis:

- Procedure Errors are procedures for performing the required function that are incomplete, inaccurate, or incorrect.
- Data Entry Errors entail data that was incorrectly input.
- Maintenance Errors entail procedures that were not followed.
- Management Errors are cases in which management made an improper decision.
- Technical Specification Problems entail technical specifications that were incomplete, confusing, or conflict with each other.
- V&V Errors entail procedures that were not thoroughly reviewed against requirements and technical specifications or verified.
- Analysis Errors are failures in analyzing the requirements, resulting in incomplete or incorrect designs and procedures.
- Requirement Problems are problems with requirements such as inconsistentency or incompleteness.

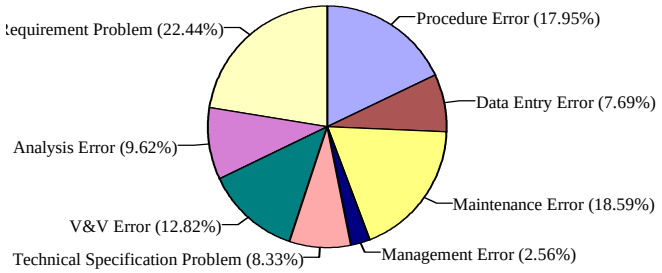

Figure 7. Digital HSI Errors

Examination of the data to determine where problems with surveillances occurred provides the results shown in Figure 8. According to the data, of the 93 surveillance errors 14 occurred in digital hardware, 21 in the software, and 58 in the HSI.

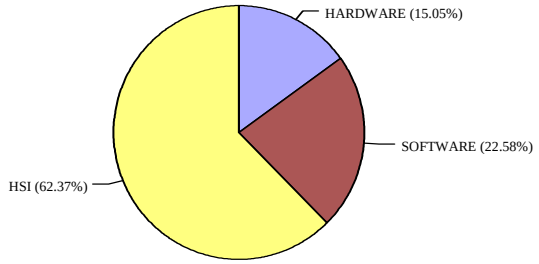

Figure 8. Digital Surveilance Problems

The types of surveillance problems that occurred were broken down into five different categories: 1) test error; 2) design error; 3)Function or box partially not tested 4) Occurred during test, and 5) surveillance missed. The results are shown in Figure 9.

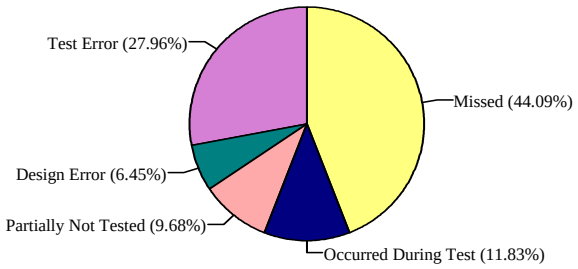

Figure 9. Surveilance Problem Breakdown

CONCLUSIONS

This section presents observations made from this database study.

The first observation indicates that some I&C components in non-safety systems have risk-significance. The second observation suggests a closer look at I&C components embedded in safety systems. Often, the scope of safety I&C components is limited to reactor protection systems and engineered safety features actuation systems. However, many safety systems and components, such as pumps, valves, and diesel generators, depend upon I&C components to function correctly. The third observation points to the possible risk-significance of embedded I&C components in breakers, inverters, and other required power supply components for both safety and non-safety systems. The final observation shows design and maintenance errors having as much impact on I&C reliability as component failure.

Based upon the analysis of the LER database, the failure of digital systems affects plant performance and safety. The analysis has shown that digital systems are involved with approximately 9% of the events reported in LERs and contribute approximately 13% of the trips. Analysis of the LER database reveals the types of problems occurring with digital I&C system installation and usage. However, the data is of insufficient depth to perform a definitive risk analysis. Perhaps one of the most significant observations is that with the use of computers, the problems encountered are caused by poor design, incomplete implementation of the system requirements and the human tendency to believe what the computer shows them. The other major failure category is in the V&V, both in incompleteness at the requirements level and during the V&V process. A significant number (93) of the LERs were attributed to missed surveillances. In many of these LERs, the surveillance scheduling computer programs were written in such a way that they did not alert the user to the critical dates.

REFERENCES

1. USNRC, 1999, *Sequence Coding and Search System Database*, http://scss.ornl.gov/scss/default.htm This is arstricted site, and permission to access the site must be obtained from Contact Dale Yeilding (301-415-6355)at the NRC with questions or comments concerning the SCSS Web site.