A QUALITATIVE ASSESSMENT OF CURRENT CCF GUIDANCE BASED ON A REVIEW OF SAFETY SYSTEM DIGITAL IMPLEMENTATION CHANGES WITH EVOLVING TECHNOLOGY

Kofi Korsah, Michael Muhlheim
Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, TN, 37831
korsahk@ornl.gov; muhlheimmd@ornl.gov

Richard Wood
The University of Tennessee, Circle Park Dr., Knoxville, TN, 37996
rwood11@utk.edu

ABSTRACT

This paper is a summary of a study performed in support of the US Nuclear Regulatory Commission (NRC) to evaluate current policy on software common-cause failure (CCF). The study reported in this paper is one of several that contributed to the technical basis to inform NRC staff.

The study first reviewed policies and assessment guidance as discussed in the Staff Requirements Memorandum to the Secretary of the Commission, Office of the NRC (SECY) 93-087, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs,* and Branch Technical Position (BTP) 7-19, *Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,* as well as Chapter 7, "Instrumentation and Controls," in NUREG-0800, *Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants*. The study then examined instrumentation and controls (I&C) technology implementations in nuclear power plants in the light of current CCF guidance. The intent was to assess whether the current position on CCF remains appropriate given the evolutions in digital safety system implementations and, if gaps in the guidance were found, to provide recommendations as to how these gaps could be closed.

The methodology adopted was to review the vendors' technology and software implementation processes for digital safety systems as technology evolved. The following three representative safety systems were selected to provide illustrative examples:

- Eagle 21 was selected to represent vintage microprocessor-based technology used from the 1980s to mid-1990s,
- TELEPERM XS (TXS) was selected to represent second generation microprocessor-based technology used from the mid-1990s to the 2000s, and
- The advanced logic system (ALS) was selected to represent the latest trend of using technology based on field programmable gate arrays (FPGAs).

Technology implementations were reviewed in light of the basic premise of the NRC in BTP 7-19 (Revision 6), that software-based or software-logic-based digital system development errors are a credible source of CCF and therefore are susceptible to CCF because identical copies of the software-based logic and architecture are present in redundant divisions of safety-related systems. BTP 7-19 categorizes firmware and logic developed from software-based development systems all under software.

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan). Please ensure that funding programs and facilities are properly acknowledged. This helps DOE to track the impact of federally-supported research. See https://portal17.ornl.gov/pts/SitePages/Home.aspx for additional details.1

1 INTRODUCTION

1.1 Background

The US Nuclear Regulatory Commission (NRC) regulations require licensees to incorporate adequate protection against software common-cause failure (CCF) into a nuclear power plant (NPP), as well as an overall safety strategy to ensure that NPP anticipated operational occurrences and design basis events do not adversely impact public health and safety. Those protective measures can be provided through diverse functions and systems.

The NRC initiated a study at ORNL to establish the technical basis on which to develop a digital systems CCF rule. This rulemaking would review and modify or affirm the NRC's current digital system CCF policy as discussed in the Staff Requirements Memorandum to the Secretary of the Commission, Office of the NRC (SECY) 93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs, and Branch Technical Position (BTP) 7-19, Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, as well as Chapter 7, "Instrumentation and Controls," in NRC Regulatory Guide (NUREG)-0800, Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants (ML033580677).The Oak Ridge National Laboratory (ORNL) is providing technical support to the NRC staff on the CCF rulemaking, and this report is one of several providing the technical basis to inform NRC staff members.

1.2 Scope of Study

To support the CCF rulemaking project, this study examined the evolutions of technology and software implementation strategies from the 1990s to the present with regard to safety system development and in light of current regulatory guidance on CCF. Key issues examined during the study include the following questions regarding evolutions in technology and software implementations:

a. What is NRC's current position on CCF?
b. Is the current position adequate given the evolutions in digital safety system implementations from the 1980s to date? What are the gaps in the current NRC position where the move from the old single board computer technology to FPGA technology is not being addressed?
c. If the current guidance is not adequate, what should be done to make it acceptable?

The methodology adopted was to review the vendors' technology and software implementation processes for digital safety systems as technology evolved. The following three representative safety systems were selected to provide illustrative examples:

- Eagle 21 was selected to represent vintage microprocessor-based technology used from the 1980s to mid-1990s,
- TELEPERM XS (TXS) was selected to represent second generation microprocessor-based technology used from the mid-1990s to the 2000s, and
- The advanced logic system (ALS) was selected to represent the latest trend of using technology based on field programmable gate arrays (FPGAs).

2 STUDY FINDINGS

2.1 Current Regulatory Position on CCF

Current regulatory guidance on digital CCF is discussed in SECY 93-087 [1] and in BTP 7-19 [2]. On the basis of experience in digital instrumentation and control (DI&C) reviews, NRC staff members also established further guidance with the development of DI&C-ISG-02 [3]. However, Revision 6 of BTP 7-19 (issued July 2012) incorporates the content of DI&C-ISG-02 and is therefore the most relevant.

The basic premise in BTP 7-19 (Revision 6) is that *"*software-based or software-logic-based digital system development errors are a credible source of CCF. . . generally, digital systems cannot be proven to be error free and, therefore, are considered susceptible to CCF because identical copies of the software-based logic and architecture are present in redundant divisions of safety-related systems.*"* BTP 7-19 categorizes firmware and logic developed from software-based development systems all under software.

The NRC's guidance on defense against CCF in BTP 7-19 is provided in a four-point position, which may be summarized as follows:

- Evidence shall be provided that the DI&C system has been adequately analyzed to identify and address any vulnerabilities to CCF.
- An analysis shall be made of each postulated common-mode failure for each event evaluated in the safety analysis report (SAR), and it shall be demonstrated that adequate diversity has been provided in the design for each of these events.
- A diverse means of performing a safety function shall be provided if the safety system providing that safety function is identified as being subject to a common-mode failure.
- An independent and diverse set of displays and controls for manual, system-level actuation of critical safety functions, and the monitoring of parameters that support the safety functions, shall be provided.

Additional guidance on digital CCF is also provided in the Interim Staff Guidance DI&C-ISG-04, "Highly-Integrated Control Rooms−Communications Issues." In particular, Item 2, "Command Prioritization," of DI&C-ISG-04, provides guidelines on priority modules used to combine diverse actuation signals with the actuation signals generated by the digital system to which they are diverse [4]. The guidance in the document may be summarized from the first two paragraphs of the staff position in DI&C-ISG-04:

> *. . . the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to common-cause failures (CCF). . ..*
>
> *An applicant should demonstrate that adequate configuration control measures are in place to ensure that software-based priority modules that might be subject to CCF will not be used later for credited diversity. . . .*

2.2 Unique Characteristics of Digital Technology

The study first examined the unique capabilities and characteristics of digital technology that distinguish it from traditional analog technology, and therefore make the above assertion likely. The most relevant characteristics were found to be the following:

- ***Digital systems typically have multiple functionality***—A digital system may be designed to perform multiple functions (e.g., acquire input data, process the data, perform onboard diagnostics, monitor alarmed conditions). With today's sub-micron integrated circuit feature sizes, this usually means that all the functions could reside in a very small space. Thus, failure of one integrated circuit could result in failure of multiple functions. In addition, important functionality is often integrated into servers and processors. The implication of this is that some performance parameters such as transmission speed and response times may deteriorate with a growing size of the I&C system due to higher processing loads. This characteristic has the potential to negatively affect important plant or I&C functions such as the quality of closed loop control and reaction times of the human-system interactions.

- ***Information processing is fundamentally sequential in nature***—Analog and digital circuitry at NPPs are a means of acquiring signals from sensors and communicating the measured values to guide safety or control actions. Analog circuitry is traditionally hard-wired and dedicated to specific tasks. In contrast, digital systems signals are sampled and digitized, and the resulting information is transmitted and processed sequentially. This means that existing functional specifications such as response time and dead time must be reconsidered in detail before they are applied to the new DI&C design.

- ***The complexity of digital systems makes licensing more challenging***—When licensing DI&C, it is difficult to assure sufficient testing of the software. Even a small software module can exhibit enough complexity to make a full verification of its correctness within reasonable cost and schedule impractical. The assumption is that there is some probability that a latent error not discovered during the verification and validation (V&V) process may disrupt its function in a crucial situation. In this scenario, building (software) redundancy into the system cannot remedy the situation because the software is deterministic in its operation, and each redundant channel will have the same embedded error. Even the use of software diversity cannot guarantee adequate protection against such potential for CCF because the requirement specification may be the ultimate cause of a software error. In essence, a (complex) digital system is fundamentally non-linear, so it is difficult to model and/or predict its behavior.

On the other hand, additional complexity enables additional functionality that can provide substantially greater confidence in correct operation in analyzed circumstances. This is accomplished through self-checking and health monitoring. Moreover, additional capabilities of digital systems can reduce the conceptual workload of the human operators (and thereby increase the probability of taking correct actions) by providing interpreted data in more easily understood formats. The goal of the nuclear power regulatory process is to provide reasonable assurance of adequate safety. The greater confidence in correct operation offered by self-diagnostics must be balanced against the potential for digital instrumentation to contain unrevealed errors that are technically difficult to correct.

2.3 Study Findings

The findings from the review of the three representative systems are summarized as follows:

1. Early microprocessor-based safety system implementations such as the Eagle-21 process protection system was designed as a modular *functional replacement for existing analog equipment*. Starting from the premise that analog systems were mature technologies and their review processes were stable, a strict adherence to digital functional replacement for existing analog equipment was seen as limiting the potential for digital CCF. This appears to be the baseline upon which subsequent guidelines such as BTP 7-19 and the DI&C ISG were developed. This is a reasonable baseline, and although it is not quantitative, the authors believe that the state of the art does not currently warrant

using any quantitative approach.

2. Although early digital implementations were typically one-for-one replacements of the proven analog designs as exemplified by the Eagle 21, some advantages of digital technology (e.g., onboard diagnostics) were nevertheless also implemented. For example, the Eagle 21 implemented automatic surveillance testing (to reduce the time required to perform surveillance tests), self-calibration (to eliminate rack drifts and time consuming calibrations), and self-diagnostics (to reduce the time required for troubleshooting). The drawback of implementing these software enhancements was the need to assure deterministic software behavior in spite of the additional software overhead. In the Eagle 21, deterministic performance was implemented as follows;

    a. Use a modular approach in the software design, with all executable code contained in modules or subroutines.

    b. No interrupts are allowed.

    c. No re-entrance is allowed.

    d. Code format conforms to standards for both high-level and assembly language routines

    e. GO TO statements are not allowed.

    f. All modules are single task (no operating system or multi-tasking system).

    g. All modules are single entry, single task.

    h. Modules exit to points of call

    i. Each module has a design performance specification and a verification test specification. However, these implementations alone do not necessarily guarantee sufficient determinism. For example, with the added overhead of onboard diagnostics and surveillance software, each module, as well as each complete cycle, should also be guaranteed to complete in a pre-determined time.[a]

3. The software V&V and digital communication standards and guidelines available in this period (i.e., in the era of the Eagle 21) were generally adhered to in the system development. Since then, there have been considerable improvements in these standards and guidelines (e.g., DI&C-ISG-02) which now address issues such as interdivisional communication. However, because the early digital safety system implementations tended to be one-for-one replacements of analog systems with no inter-divisional communication, etc., the early standards and guidelines were adequate for the period.

4. Evolution of safety system implementations made use of more sophisticated microprocessors and increased online self-testing and surveillance, as exemplified by the TXS. However, these systems (TXS) also made use of the improving guidance for digital safety system implementations (e.g., updated V&V standards) and improved on implementation of deterministic performance. For example, the digital system architecture of the TXS included procedures that improved determinism such as (a) monitoring of cycle time by means of software and a hardware watchdog, (b) automatic testing of the watchdog, (c) bus systems with constant load, and (d) no processing of absolute time or date. Improvements in safety system software also included self-testing of the inputs from the input modules and automatic readback of the outputs from the output modules.

5. Because digital safety system implementations were also accompanied with improvements in regulatory guidance, the issue of CCF was also a greater focus in safety systems implemented

[a] It is possible that this was also implemented in the early digital software safety systems such as the Eagle 21. However, the authors were unable to ascertain this from the available documentation.

beginning in the mid-1990s to the 2000s. For example, the preferred measure against CCF, especially in connection with design errors, was functional diversity. This involves ensuring that the safety I&C subsystems, while equipped with the same hardware and system software, execute different I&C functions for handling one and the same event. For example, a reactor trip resulting from a steam generator tube rupture event may be monitored by two I&C subsystems: one monitoring main steam activity, and one monitoring steam generator level and pressurizer level. The assumption here is that the same hidden fault will not take effect simultaneously in two different functions at the same time, causing both of them to fail simultaneously. In the absence of a quantitative measure, BTP 7-19 and DI&C-ISG-04 provide good additional guidance for addressing digital CCF.

6. Software V&V procedures, reviews, and audits are important parts of the effort to reduce the potential for CCF and to comply with NRC requirements. The review of software V&V procedures for safety system implementations showed that there were general improvements in software V&V as the technology implementations also evolved. However, these improvements resulted from updates and improvements in regulatory guidance as well as from technology evolutions. The revisions to regulatory guidance resulted from updates and improvements in the standards endorsed by the regulatory guides. For example, the 2013 version of RG 1.168, "Verification, validation, reviews, and audits for digital computer software used in safety systems of NPPs," has undergone a significant update as a result of revisions of the endorsed standards in the 1997 version. (The latter version was used to guide V&V for the TXS reviewed for this report). Examples include the addition of a security analysis and the recommended use of the software integrity system, as the previous version did not require the selection of an integrity level.

7. With regard to the migration to FPGA technology, the reviews did not show that common cause failures are any less plausible for FPGA-based safety systems than for microprocessor-based safety systems. For both FPGA-based systems and microprocessor-based systems, it is difficult to prove adequate test coverage. Thus, the method of ensuring adequate quality of the product continues to be extensive documentation of the development process, qualification, testing, guidelines on how to address computer communication issues (DI&C-ISG-04), guidelines on how to address diversity and defense-in-depth issues (BTP 7-19 Rev 6), etc. In the absence of quantitative methodologies (which the present state-of-the-art do not support), the current standards and guidelines provide very good guidance to assure quality and reduce the potential for CCF in DI&C for NPPs and should continue to be applied.

3 CONCLUDING REMARKS

The review of software V&V procedures showed that for safety system implementations there were general improvements in software V&V as the technology implementations also evolved. However, these improvements resulted from updates and improvements in regulatory guidance as well as from technology evolutions. The revisions to regulatory guidance resulted from updates and improvements in the standards endorsed by the regulatory guides.

With regard to the migration to FPGA technology, the reviews did not show that common cause failures are any less plausible for FPGA-based safety systems than for microprocessor-based safety systems. For both FPGA-based systems and microprocessor-based systems, it is difficult to prove adequate test coverage, and the method of ensuring adequate quality of the product continues to be extensive documentation of the development process, qualification, testing, and guidelines on how to address computer communication issues

In the absence of quantitative methodologies (which the present state-of-the-art do not support), the current standards and guidelines provide very good guidance to assure quality and reduce the potential for CCF in DI&C for NPPs and should continue to be applied.

In conclusion, current guidance aimed at reducing the potential for CCF as found in BTP 7-19 (Rev. 6) and DI&C-ISG-04 should continue to be relied upon. Operational experience could also be investigated in a future study to support current guidance. Operational experience alone cannot be used as proof of adequate design against CCF: the (safety) system may have been operating well for years during which the plant may even have undergone abnormal conditions showing that it performed its safety function under those abnormal conditions. However, that does not necessarily demonstrate adequate functionality under all scenarios that may not have occurred during the plant's operation.

ACKNOWLEDGEMENT

This paper is a summary of work performed under contract with the U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (NRR/DE/EICB). The authors acknowledge NRC project manager Rossnyev Alvarado and ORNL project manager Gary Mays for their guidance.

REFERENCES

1. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993 (ADAMS Accession No. ML003708056).

2. BTP 7-19, Rev. 6, "Guidance for Evaluation of D3 in Digital Computer-Based Instrumentation and Control Systems," US NRC, July 2012. (ADAMS Accession No. ML110550791)

3. DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues Interim Staff Guidance," Revision 2, June 2009.

4. DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues," Interim Staff Guidance Revision 1, March 2009.