STRATEGIES FOR DIVERSITY USAGE TO MITIGATE POSTULATED COMMON CAUSE FAILURE VULNERABILITIES

Richard T. Wood
Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA 37831-6010
WoodRT@ornl.gov

Michael E. Waterman
U.S. Nuclear Regulatory Commission
Washington, District of Columbia, USA 20555
Michael.Waterman@nrc.gov

ABSTRACT

This paper describes an approach to establish effective mitigating strategies that can resolve potential common-cause failure (CCF) vulnerabilities in instrumentation and control systems at nuclear power plants. A particular objective in the development of these strategies, which consist of combinations of diversity attributes and their associated criteria, is to address the unique characteristics of digital technology that can contribute to CCF concerns. The research approach employed to establish diversity strategies involves investigation of available documentation on diversity usage and experience from nuclear power and non-nuclear industries, capture of expert knowledge and lessons learned, determination of common practices, and assessment of the nature of CCFs and compensating diversity attributes. The resulting diversity strategies address considerations such as the effect of technology choices, the nature of CCF vulnerabilities, and the prospective impact of each diversity type. In particular, the impact of each attribute and criterion on the purpose, process, product, and performance aspects of diverse systems are considered.

INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) has established regulatory guidance addressing a method for assessing the diversity and defense-in-depth (D3) provided by the instrumentation and control (I&C) system architecture at a nuclear power plant (NPP). This method enables determination of whether vulnerabilities to common-cause failure (CCF) have been adequately addressed. The guidance is included in Branch Technical Position 7-19, “Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems” (NRC, 2007a), within Chapter 7, “Instrumentation and Controls,” of NUREG-0800, *Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants* (NRC, 2007b). This guidance provides a method for determining the need for diversity. However, there is currently no definitive guidance specifying how much diversity is sufficient to mitigate CCF vulnerabilities that may arise from digital safety system designs. Consequently, Oak Ridge National Laboratory has engaged in research to

establish effective mitigating strategies that address the unique characteristics of digital technologies that contribute to the potential for CCF. The specific objective of this research effort was to identify and develop diversity strategies, which consist of combinations of diversity attributes and their associated criteria, by leveraging the experience and practices of other industries and the international nuclear power community. Effectively, these baseline sets of diversity criteria constitute suitable mitigating diversity strategies that adequately address potential CCF vulnerabilities in digital safety-related I&C systems. The strategies are suitable for use in design reviews as comparative templates or guides to support evaluation of diversity usage to resolve CCF vulnerabilities that have been identified via a D3 analysis.

Background

NRC regulations require licensees to develop an overall safety strategy for defense-in-depth functions and systems to ensure that abnormal operating occurrences (AOOs) and design basis accidents do not adversely impact public health and safety. In particular, the design criteria for NPP safety systems embody principles such as high quality, integrity, reliability, independence, and qualification. Separation and redundancy, physical barriers, and electrical isolation are generally applied as design measures to address potential vulnerabilities related to a single failure of equipment and the propagation of failure effects. These measures tend to minimize shared components or equipment and nonessential interconnections within I&C system architectures. Nevertheless, the potential for CCF vulnerability has long been recognized and diversity is therefore employed as a contributing factor in satisfying safety requirements. For example, the failure of reactor trip functions, which would require the concurrent failure of more than one redundant channel or division in a reactor trip system, is addressed through regulatory requirements for provision of diverse equipment/systems to respond to anticipated transients without scram (ATWS).

The general design criteria (GDC) provided in Appendix A of Title 10, Part 50 of the Code of Federal Regulations (10 CFR 50) (CFR, 2004) establish the minimum design requirements for light-water reactors. The introduction to Appendix A explicitly states that “the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems” needs to be considered. Several of the GDC for protection systems deal with issues that are relevant to mitigation of potential CCF vulnerabilities. In particular, GDC 22 requires that “functional diversity or diversity in component design and principles of operation … be used to the extent practical to prevent loss of the protection function.”

The consequence of these regulatory requirements is that diversity approaches, such as the combination of functional and signal diversity, have been extensively employed for conventional (i.e., hardwired) safety systems. These “traditional” diversity strategies remain effective in addressing criteria such as GDC 22. However, the increased potential for CCF vulnerability posed by the unique characteristics of digital technology warrants consideration of additional diversity usage to supplement the traditional diversity strategies.

Detailed guidance on the method for performing D3 analyses of reactor protection systems to identify appropriate diverse systems and defense-in-depth approaches is provided in NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems* (NRC, 1994). The primary goal of the D3 analysis is to determine where diversity may be needed to mitigate the potential adverse effects of CCF vulnerabilities. Limited guidance is provided on the means for establishing sufficient diversity to resolve the vulnerabilities.

Diversity is characterized in NUREG/CR-6303 in terms of attributes and criteria. Specifically, NUREG/CR-6303 separates diversity attributes into the following six areas to facilitate assessments of adequate diversity in safety systems:

- Design diversity,
- Equipment diversity,
- Functional diversity,
- Human diversity,
- Signal diversity, and
- Software diversity.

The guidance on diversity in NUREG/CR-6303 provides a set of recommended criteria for each of the six diversity attributes. However, the number of criteria in each attribute, coupled with the number of attributes, creates a sizable and complex collection of possible combinations of attributes and criteria that could be used to achieve adequate diversity in a safety system, making the guidance difficult to use as a design assessment tool. As a result, comprehensive guidance and objective acceptance criteria to resolve the efficacy of separate or combined diversities (or other defensive design approaches) and thus provide an effective, optimal approach to addressing (e.g., avoiding or mitigating) CCFs have been needed. Primarily, the objective of the research focused on addressing two issues: (1) determining how much diversity is required and (2) identifying what combinations of diversities are most effective in avoiding CCF vulnerability.

Research Approach

Because of the complexity of digital I&C system technology and the necessary reliance on process-driven approaches to software development and quality assurance, there has been an absence of definitive quantitative measures for key digital I&C system characteristics. As a result, it has not been feasible to develop a comprehensive measure of diversity (particularly for software-based systems) that could be used to establish wholly objective acceptance criteria to support diversity reviews. However, the findings of this research enable effective diversity strategies to be defined based on the diversity attributes of NUREG/CR-6303 and consensus practices and experience within other application domains.

The research effort began with an investigation of available documentation on diversity approaches and experience from international nuclear power and other industries. Nonnuclear industries and organizations were investigated to determine their approaches to and experience with avoiding or mitigating the effects of CCF in high-

integrity and/or safety-significant systems. This investigation focused on industries that employ similar I&C technologies and have high-consequence applications. The findings address the aerospace, aviation, chemical process, and rail transportation industries. Key organizations include the National Aeronautics and Space Administration (NASA), the Federal Aviation Administration, the Center for Chemical Process Safety (CCPS) and the Federal Railway Administration. Since the nonnuclear, high-failure-consequence industries studied have transitioned to digital control systems, the use of D3 strategies for CCF avoidance and/or mitigation is of particular relevance as a basis for devising nuclear power–specific guidance on diversity.

For the nuclear power industry, the extensive application of digital technology in I&C systems at international evolutionary NPPs provides a significant resource to support this effort to establish effective strategies for addressing CCF vulnerabilities. A focused study of international NPPs was conducted to ascertain distinct diversity approaches for consideration in developing CCF coping strategies. Diversity approaches evaluated included Sizewell NPP in the United Kingdom, Darlington NPP in Canada, Chooz NPP in France, Ulchin NPP in Korea, Temelín and Dukovany NPPs in the Czech Republic, and Kashiwazaki-Kariwa NPP in Japan, as well as the D3 strategies being implemented at Lungmen NPP in Taiwan and Olkiluoto NPP in Finland.

The research approach for establishing diversity strategies involved capturing expert knowledge and lessons learned, determining best practices, and assessing the nature of CCFs and compensating diversity attributes. The basis for these strategies centers on practices derived from examples of diversity usage by the international nuclear power industry and several nonnuclear industries with high-integrity and/or safety-significant I&C system implementations. The approaches to diversity identified from international NPPs serve as representative examples of the strategies. While the examples identified from nonnuclear industries are relevant because of the safety significance of the functions and the use of comparable technology, context differences in the usage domains limit their direct applicability. Thus, key insights are derived from these examples to inform the development of diversity strategies in this research. The resulting diversity strategies address considerations such as the effect of technology choices, the nature of CCF vulnerabilities, and the prospective impact of each diversity type.

The diversity strategies developed through this research are composed of combinations of diversity criteria that are adapted from the attributes and criteria defined in NUREG/CR-6303. When it was published in 1994, computer-based digital systems were assumed to comprise the next generation of safety systems. More recent safety system designs using programmable logic devices, field programmable gate arrays (FPGAs), application-specific integrated circuits, and multi-aperture magnetic ladder-like logic structures (Laddic) required revisions to the diversity attributes to ensure the diversity criteria could be applied independent of the technology used to implement a safety system design. Consequently, the Equipment diversity attribute was divided into two attributes, Equipment Manufacturer and Logic Processing Equipment. The Logic Processing Equipment diversity attribute criteria were renamed to better represent different technologies. Additionally, the Software diversity attribute was renamed the Logic diversity attribute to better reflect differences in logical representations of system

functions, and the associated criteria were renamed to reflect differences in the manner logic could be instantiated in a system. The resulting Equipment-related and Logic-related attributes and criteria are shown in Figure 1.

Figure 1. Diversity attributes and associated criteria derived from NUREG/CR-6303.

NATURE OF COMMON-CAUSE FAILURE

CCF is defined by the International Atomic Energy Agency (IAEA) as a “failure of two or more structures, systems or components due to a single specific event or cause” (IAEA, 2005). The International Electrotechnical Commission (IEC) further adds to the CCF definition by noting that the “coincidental failure of two or more structures, systems or components is caused by any latent deficiency from design or manufacturing, from operation or maintenance errors, and which is triggered by any event induced by natural phenomenon, plant process operation, or action caused by man or by any internal event in the I&C system” (IEC, 2008). CCF is a class of dependent failures in which the probability of failure is not expressible as the simple product of the unconditional failure probabilities of the individual events.

Latent faults can originate at any phase of the digital I&C system life cycle; are typically human induced or technology related; and involve design flaws, performance limitations, or implementation complexity. At a high level, three prominent sources of latent systematic faults are (1) errors in the requirement specification, (2) inadequate provisions to account for design limits (e.g., environmental stress), and (3) technical faults incorporated in the internal system (or architectural) design.

Triggering conditions that can activate faults and result in failure arise primarily from human actions, signal trajectory, external events, and temporal effects. Human actions can include maintenance errors, input mistakes, out-of-sequence commands, and ill-timed or conflicting actions. The signal trajectory for a digital I&C system involves not only current input values but also past input values, the internal state of the system, and the sequence of transitions among internal states. The IEC defines signal trajectory as the "time histories of all equipment conditions, internal states, input signals and operator inputs which determine the outputs of a system" (IEC, 2006).

USAGE OF DIVERSITY

As previously noted in the research approach description, an investigation was conducted of diversity practices and usage experience within the international nuclear power industry and for several nonnuclear industries. The goal of this investigation was to identify approaches for the treatment of the potential of CCF in high-integrity and or safety-significant I&C systems. Significant examples of diversity usage were found in each application domain. These representative cases are summarized below. In addition, the cited examples of diversity usage are described in detail in NUREG/CR-7007, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems* (NRC, 2009).

International Nuclear Power Industry

When microprocessor-based safety systems were first introduced in the 1980s, the nuclear power industry recognized the prospect for significant CCF vulnerability among digital systems in which identical software is executed on identical hardware. The nuclear power industry's approach to addressing the potential for CCF vulnerability in a digital protection system consists of some of the most extensive and regulated practices found among the industries studied in this investigation. The diversity attributes and analysis guidance documented in NUCREG/CR-6303 were developed concurrently with the first extensive applications of digital technology for international evolutionary reactors. Consequently, the investigation of diversity usage in the nuclear power industry concentrated on example cases at international NPPs.

The examples described in this section represent a sampling of evolutionary reactors and modernized plants that employ digital technology extensively. In particular, six of the earliest examples of highly integrated digital I&C systems that have been implemented at new installations were included in the survey. These plants are Darlington, Sizewell, Chooz, Kashiwazaki-Kariwa, Temelín, and Ulchin. An example of extensive modernization for an existing plant (Dukovany) based on digital I&C technology was investigated as well. Finally, two plants currently undergoing licensing

and construction were studied to assess recent trends. These plants are Lungmen and Olkiluoto.

For evolutionary NPPs with significant use of digital systems, a common diversity usage approach involves a systematic subdivision of the protection functions into versions A and B and an assessment of the degree of diversity between the two versions based on a pair-wise comparison of the individual mitigation characteristics. The result is identification of the categories of the diversity attributes that can be used to show that the diverse systems do not have some common vulnerability that could cause a protective function to fail. Most of the plant architectures for I&C systems that were identified in the investigation make the claim of diversity, but they differ in overall approach. The approaches to diversity usage in the reported case histories can be grouped into three broad categories: coequal diverse systems, primary/secondary diverse systems, and functionally diverse subsystems. Of these examples, functional diversity is the most common.

In the architectural approach identified as coequal diverse systems, diversity is achieved between two separate safety systems that provide equivalent protective action. This approach is illustrated in Figure 2. Systems A and B represent two diverse systems, each of which processes data to generate commands. The input data are generally provided through separate paths and are often from different (possibly diverse) sources for the two systems. Likewise, the commands (i.e., actuation signals) from each system are transmitted across separate paths to actuation devices that are generally different and may be diverse. Either system can independently initiate an equivalent safety action in response to a detected event. Although the two systems typically drive separate actuation devices, their collective action can be seen as a virtual “OR” providing one-out-of-two logic. In most cases, systems A and B are treated according to the highest safety class and both can provide full coverage against all design basis events (DBEs), including normal and abnormal operating events as well as design basis accidents. The systems typically are separate from end to end (including sensors and actuators) and do not share any intersystem communication link. The diversification of the systems is also generally applied across the board (e.g., signals, platforms, functions, actuation mechanisms).

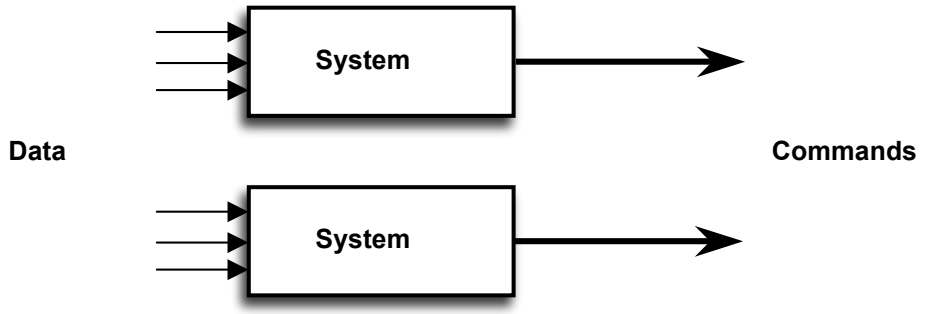

Figure 2. Coequal diverse safety systems.

The architectural approach identified in terms of primary and secondary diverse systems is similar to the coequal diverse safety system approach in that the diverse systems are primarily treated as separate systems. A key distinction is that the secondary system is not equivalent to the primary system in some sense (e.g., classification or functionality). Figure 3 illustrates the approach. In this discussion, System A is treated as the primary system (i.e., primary safety system) while System B is treated as the secondary system (i.e., backup system). Many of the considerations identified above will hold true for this architectural approach. The commands for each system may remain separate to drive different actuation devices as above (shown as a dotted line in this figure), or they may combine through logic voting or a priority module to drive the same actuation device. The distinction between the primary and secondary systems is generally seen in terms of the coverage of postulated initiating events and/or the safety classification. Specifically, the secondary system may only provide backup safety or compensating functions for high-frequency DBEs, such as AOOs. This can be seen in NPP examples of reduced functionality backups such as secondary safety systems or ATWS systems. The other principal distinction between the diverse systems is the use of a lower safety class or nonsafety system to serve as the secondary diverse system. Diverse actuation systems (DASs) and ATWS systems are examples of this distinction with the primary/secondary approach.

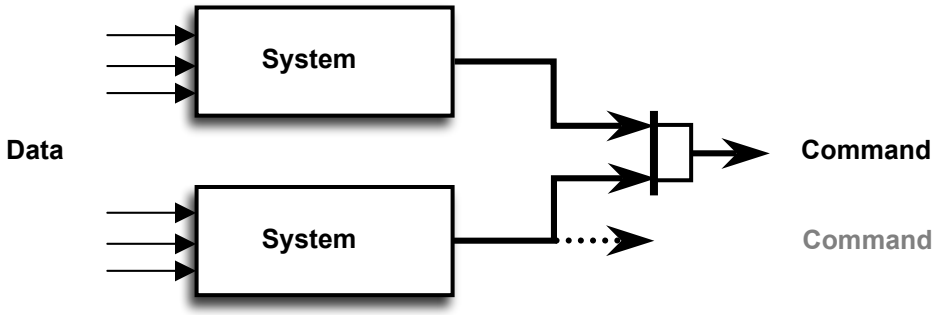

Figure 3. Primary and secondary diverse systems.

The functionally diverse subsystem architectural approach involves the strategic use of functional diversity combined with signal diversity. Diversification of this form can be applied alone within a single safety system or in conjunction with the other architectural approaches described above. The unique characteristic of this approach is that two diverse versions are implemented as subsystems rather than separate systems. Figure 4 illustrates this architectural approach. It is shown as two safety systems (or, more commonly, two redundancies within one safety system) that each have two subsystems. The collection of “like” subsystems A or B constitutes a line of protection (1 or 2) within the overall safety system, which is composed of the two (or more) redundancies. In practice, there will likely be three or four redundancies, with each containing the two distinct subsystems. The commands (e.g., partial trips) from each instance of a subsystem type (A1, A2, etc., or B1, B2, etc.) are voted to determine the resultant safety decision for the individual line of protection (1, 2, etc.). The actuation

commands from the lines of protection can be transmitted directly to separate trains of actuators or can be further combined through downstream coincidence or priority logic.

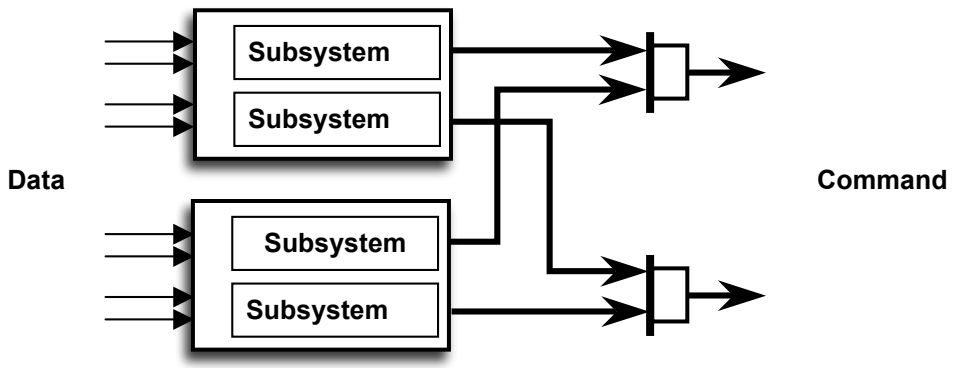

Figure 4. Functionally diverse subsystems.

Table 1 summarizes the diversity usage identified through the investigation of the international evolutionary NPPs. The findings are given for Darlington, Sizewell, Chooz, Kashiwazaki-Kariwa, Temelín, Ulchin, Dukovany, Lungmen, and Olkiluoto. The prevalent approach to implementing diversity is through an architecture based on primary and secondary diverse systems, with at least one of those systems incorporating traditional functional diversity supported by signal diversity. Most examples studied involved implementations of microprocessor-based platforms as the basis for each diverse system.

Nonnuclear Industries

A variety of nonnuclear industries were investigated during the course of this research. Many were found to rely primarily on high-quality processes and rigorous hazard identification and resolution. The investigation identified different approaches that ranged from no diversity (e.g., the almost total reliance on redundancy of high-quality modules and defense-in-depth layers with no “intentional” diversity) to minimal diversity (e.g., reduced functionality backups with limited diversity) to more extensive diversity (e.g., combinations of techniques for fault management addressing high-consequence failures with “encouraged” but not fully specified diversity). Four industries in particular were found to have guidance related to CCF mitigation or provided clear examples of diversity usage. The application domains that provided the most significant information are the aerospace, aviation, chemical process, and rail transportation industries.

Table 1. Summary of diversity usage for international nuclear power plants[a]

Diversity attribute	Nuclear power plant[b]								
	Dr	S	C	K	T	U	Dk	L	O
Design									
Different technologies	–	x	–	x	–	–	–	–	–
Different approach—same technology	–	–	–	–	–	–	–	–	x
Different architectures	x	i	x	i	x	x	–	x	i
Equipment Manufacturer									
Different manufacturer—different design	–	x	–	–	–	–	–	–	–
Same manufacturer—different design	–	–	–	–	–	–	–	–	x
Different manufacturer—same design	x	–	x	–	–	–	–	x	–
Same manufacturer—different version	–	–	–	x	x	x	–	–	–
Logic Processing Equipment									
Different logic processing architecture	x	i	x	i	x	x	–	x	i
Different logic processing versions in same architecture	–	–	–	–	–	–	–	–	–
Different component integration architecture	x	i	–	–	x	x	–	x	i
Different data-flow architecture	–	i	–	–	x	–	–	x	i
Functional									
Different underlying mechanisms	x	i	–	i	–	–	–	–	i
Different purpose, function, control logic, or actuation means	x	x	x	x	x	x	x	x	x
Different response time scale	x	–	–	–	–	–	–	–	–
Life Cycle									
Different design organizations/companies	–	x	x	–	–	–	–	x	–
Different management teams within same company	x	–	–	–	x	x	–	–	x
Different design/development teams (designers, engineers, programmers)	x	i	i	–	x	x	–	i	x
Different implementation/validation teams (testers, installers, or certification personnel)	x	i	i	–	x	x	–	i	x
Logic									
Different algorithms, logic, and program architecture	x	i	x	i	x	x	x	x	x
Different timing or order of execution	–	i	–	i	–	–	–	x	i
Different runtime environment	x	i	–	i	–	–	–	–	i
Different functional representation	x	i	–	i	x	–	–	–	i
Signal									
Different parameters sensed by different physical effects	x	x	x	x	x	x	x	x	x
Different parameters sensed by same physical effects	x	x	x	x	x	x	x	x	x
Same parameter sensed by different redundant set of similar sensors	x	x	x	x	x	x	x	x	x

[a]Intentional diversity (x), inherent diversity (i), not applicable or no information (–).

[b]Dr = Darlington, S = Sizewell, C = Chooz, K = Kashiwazaki-Kariwa, T = Temelin, U = Ulchin, Dk = Dukovany, L = Lungmen, and O = Olkiluoto.

The aerospace industry tends to rely on high-quality processes to minimize the potential for CCF vulnerabilities. The flight control system of the Space Shuttle or Space Transportation System and the station command and data handling system of the International Space Station (ISS) provide prominent examples of safety-critical I&C applications for human-rated space missions. Redundancy, fault tolerance, and backup use of human operators are primary means by which NASA supplements adherence to rigorous quality assurance practices to achieve highly reliable systems. In particular, the ISS and Space Shuttle use reduced functionality backup systems as a means for improving the probability of mission success in the event of primary software failure. Thus, the prime examples of safety-critical applications for manned space systems are characterized by the use of failsafe design practices, which includes reduced functionality backups to provide a form of functional diversity.

The aviation industry provided several examples of diversity usage. In particular, aircraft manufacturers Airbus Industrie and Boeing provide the most extensive examples for digital fly-by-wire (FBW) flight control systems (FCSs) that have been developed for the commercial aviation industry. Airbus A320, in which the overall FCS is composed of diverse redundant primary and secondary control systems, serves as one of the earliest implementations. Successor Airbus flight controllers (e.g., A340, A380) and the Boeing 777 FCS were also investigated to capture the evolution of diversity usage in modern FBW systems. The study found two prominent approaches of diversity (or dissimilarity) usage for FCS implementations. The Airbus approach emphasized diversity of development teams and software, while the Boeing approach emphasized diversity of hardware and implementation tools. The fact that each organization included microprocessor diversity as part of their practice for diversity usage serves as a significant finding given the constraints on the implementation (size and weight) and the potential burden on maintenance in the field. It is noted that the nature of the application domain favors much different architectural approaches from what is generally employed within the nuclear power industry.

The chemical process industry provides guidance that is similar in nature to the nuclear power industry. In particular, the CCPS *Guidelines for Safe Automation of Chemical Processes* (CCPS, 1993) provides the most extensive guidance on design practices for safety-instrumented systems. However, no definitive metrics or specific diversity usage template is provided. Specific applications and particular company guidelines based on the principles established by the CCPS are proprietary and not generally available. Thus, the investigation of diversity usage in the chemical process industry focused on the practices found in the CCPS guidance. The nature of the chemical process industry tends to result in separated safety loops for localized processes rather than more plant-wide monitoring and protective action as is the case for NPPs. Thus, direct translation of diversity usage from that industry, even if specific examples were available, would be somewhat limited.

The rail transport industry also provided several examples of diversity usage. Early implementations of digital train control systems relied primarily on software diversity. The Elektra railway interlocking control system of the Austrian Federal Railways provides a key example of the software-based approach. This approach, known as the safety bag technique, involves a diverse application on an independent computer to

confirm the safety characteristics of commands from the primary control application and enforce a safety envelope. A more hardware-oriented approach, which involves encoded processors, for parallel checking architectures was also seen in key examples. Two featured examples are the Système d'Aide à la Conduite, à l'Exploitation et à la Maintenance (SACEM) fault-tolerant train speed control system for the Paris Rail line A and the Vital Framework developed for the Los Angeles Metro Green Line. Essentially, an encoded processor serves as a hardwired comparator to confirm the proper execution of the safety or control function by the primary system through comparison of expected (i.e., pre-determined) properties of the code against observed or generated properties of the code. However, direct application of the approaches employed in the rail transport industry would depend on adaptation of system architectures that are significantly different from those employed in the nuclear power industry.

Table 2 summarizes the diversity usage identified through the investigation of the nonnuclear industries. Findings are given for the Space Shuttle, ISS, Airbus A320, Airbus A340, Airbus A380, Boeing 777, CCPS, Austrian Federal Railway, Paris Rail Line A, and Los Angeles Metro Green Line. For the nonnuclear diversity usage examples identified through the investigation, the primary diversities cited for establishing sufficient application independence are functional, signal, software, and life cycle (associated with the application software). While specific examples of diversity usage have been noted in other industries, little explicit guidance was found and infrequent dependence on diversity was generally observed. The less-common utilization of diversity as a mitigating strategy for several nonnuclear industries appears to be driven by considerations such as fundamental reliance on high-quality practices and procedures within an application domain, the nature of the applications and behavior of the processes, implementation constraints (e.g., size, weight, power, and cost), and acceptability of some risk.

Table 2. Summary of diversity usage in applications from nonnuclear industries[a]

Diversity attribute	Application[b]									
	SS	IS	20	40	80	77	C	A	PR	LA
Design										
Different technologies	–	–	–	–	–	–	–	–	–	–
Different approach—same technology	–	–	–	–	–	–	–	–	x	x
Different architectures	–	–	x	x	x	x	x	–	i	i
Equipment Manufacturer										
Different manufacturer—different design	–	–	–	–	–	–	–	–	–	x
Same manufacturer—different design	–	–	–	–	–	–	–	–	x	–
Different manufacturer—same design	–	–	x	–	x	–	x	–	–	–
Same manufacturer—different version	–	–	–	x	–	x	–	–	–	–
Logic Processing Equipment										
Different logic processing architecture	–	–	x	–	x	x	x	–	i	i
Different logic processing versions in same architecture	–	–	–	x	–	–	–	–	–	–
Different component integration arch.	–	–	–	–	–	–	–	–	–	–
Different data flow architecture	–	–	–	–	–	–	–	–	–	–
Functional										
Different underlying mechanisms	–	–	–	–	–	–	–	–	i	i
Different purpose, function, control logic, or actuation means	x	x	x	x	x	–	x	x	x	x
Different response time scale	–	–	–	–	–	–	–	–	i	i
Life Cycle										
Different design organizations/companies	x	–	x	–	x	–	–	–	–	x
Different management teams within same company	–	–	–	x	–	–	–	–	–	–
Different design/development teams (designers, engineers, programmers)	i	–	i	x	i	–	x	x	x	i
Different implementation/validation teams (testers, installers, or certification personnel)	i	–	i	x	i	–	x	x	x	–
Logic										
Different algorithms, logic, and program architecture	x	x	x	x	x	–	x	x	x	x
Different timing or order of execution	–	–	–	–	–	–	–	–	–	–
Different runtime environment	x	–	–	–	–	–	x	–	i	i
Different functional representation	–	–	x	x	x	x	x	x	x	i
Signal										
Different parameters sensed by different physical effects	–	–	–	–	–	–	x	x	x	x
Different parameters sensed by same physical effects	–	–	–	–	–	–	x	–	–	–
Same parameter sensed by different redundant set of similar sensors	x	–	x	x	x	–	x	–	–	–

[a]Intentional diversity (x), inherent diversity (i), not applicable or no information (–).

[b]SS = Space Shuttle, IS = International Space Station, 20 = Airbus A320, 40 = Airbus A340, 80 = Airbus A380, 77 = Boeing 777, C= CCPS, A = Australian Federal Railway, PR = Paris Rail Line A, and LA = Los Angeles Metro Green Line.

IMPACT OF DIVERSITY

The establishment of baseline diversity strategies provides guidance on suitable combinations of diversity criteria. These strategies are drawn from commonalities in identified approaches for diversity usage and technical insights into the impact of the diversity attributes and associated criteria on the potential for CCF vulnerabilities. The objective of each diversity strategy is to address sources of common faults, locations of vulnerabilities, and triggering conditions for CCFs. In terms of diverse systems, the targeted aspects related to mitigating CCF vulnerability involve purpose, process, product, and performance. The system aspects related to purpose and process concern sources by which systematic faults (e.g., flaws, deficiencies, misunderstandings, mistakes, errors, defects) are introduced. These fault sources include requirements, design concepts/system specifications, components and parts, and manufacturing lines as well as human contributors and tool sets at various life-cycle phases. The product aspect is exemplified by the realized systems, including the platforms and applications, in which latent faults reside until activated to cause a failure. The location of any common faults may involve the hardware, system software or basic processing elements, application software or logic, integrated hardware/software environment, and/or interconnections (e.g., communication, power, structure). The system aspect concerning performance includes execution of functions and responses to external influences. Execution primarily relates to demands (i.e., inputs) and processing mechanisms (e.g., internal states and state transitions) that can trigger activation of systematic faults or introduce commonalities of condition. Similar response to external influences may also serve as triggering mechanisms for common failure.

The combinations of diversity criteria that comprise each strategy can address the potential for CCF vulnerabilities by minimizing the introduction of common faults, mitigating the presence of corresponding vulnerabilities, managing commonality in usage (i.e., execution), and reducing similarity in susceptibility to external factors. The rationale for each diversity strategy is based on characterization of diversity effects in terms of impact on common systematic faults, concurrent execution profiles, or similar responses to external influences.

DIVERSITY STRATEGIES

Based on a diversity impact analysis of the findings from the diversity usage investigation, baseline combinations of diversity attributes and criteria were formulated to establish acceptable diversity strategies. To facilitate the development of the strategies, a framework for classifying strategic approaches to diversity usage was devised. Technology, which corresponds to the design diversity attribute of NUREG/CR-6303, is chosen as the principal system characteristic by which the strategies are grouped. The rationale for this classification framework involves consideration of the profound impact that technology-focused design diversity provides. Basically, instances of design diversity are readily observable and most of the other diversity attributes are strongly affected by the design/technology choice. Specifically, NUREG/CR-6303 states, “the clearest distinction between two candidate subsystems would be design diversity.”

Each of these design diversity options contribute inherent diversities that arise due to the nature of the technology and architectural differences. The degree to which the inherent diversity is provided depends on the extent of the dissimilarity between the design technologies. The use of a particular diversity criterion may be intentionally imposed in the design to support CCF mitigation or it may be achieved inherently as a consequence of the technology choice. The inherent diversities that arise due to the nature of the technology differences are identified as elements of the strategies. Greater dissimilarity between technologies results in more extensive provision of inherent diversity between designs and less need for additional intentional use of other diversity criteria.

The classification of diversity strategies developed in this research consists of three families of strategies: (1) different technologies—Strategy A, (2) different approaches within the same technology—Strategy B, and (3) different architectures within the same technology—Strategy C. Using this convention, the essential characteristics of the three strategy families are summarized as follows.

- **Strategy A** focuses on the use of fundamentally diverse technologies as the basis for diverse systems, redundancies, or subsystems. The Strategy A baseline, at the system or platform level, is illustrated by the example of analog and digital implementations providing design diversity. This choice of technology inherently contributes notable equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities. Intentional application of life-cycle and equipment manufacturer diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted. The use of a microprocessor-based primary protection system and an analog secondary protection system at the Sizewell NPP represents the principal example of Strategy A drawn from the survey findings.
- **Strategy B** involves the use of distinctly different technology approaches as the basis for diverse systems, redundancies, or subsystems. The Strategy B baseline can be described in terms of different digital technologies, such as the distinct approaches represented by programmable logic devices and general-purpose microprocessors. This choice of technology inherently contributes some measure of equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities. Intentional application of logic processing equipment, life-cycle, and equipment manufacturer diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted. The Olkiluoto diversity approach using different digital technologies [i.e., central processing units (CPUs) vs FPGAs] as the basis for the primary safety system and a diverse backup system is the principal example of Strategy B drawn from the survey findings. Nonnuclear industry examples from the rail industry employed this technology difference to implement significantly different functional approaches in a parallel arrangement of safety-critical and checking systems.
- **Strategy C** represents the use of architectural variations within a technology as the basis for diverse systems, redundancies, or subsystems. An example of the Strategy C baseline involves different digital architectures, such as the diverse microarchitectures provided by different CPUs. This choice of technology inherently

contributes some limited degree of equipment manufacturer, life-cycle, and logic diversities. Intentional application of equipment manufacturer, logic processing equipment, life-cycle, and logic diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted. The use of diverse microprocessors as the basis for primary safety systems and diverse backup systems such as ATWS or DAS constitutes the principal examples of Strategy C drawn from the survey findings. Nonnuclear industry examples primarily involve flight control systems for the aviation industry.

As noted, each of the strategy families is characterized by combinations of diversity criteria that provide adequate mitigation of potential CCF vulnerabilities when combined with the traditional diversities generally employed for conventional hardwired systems. In addition to the baseline strategy within each family, acceptable variants of each baseline were also developed. Implementation of a diversity strategy (e.g., baseline or identified variant) from any of the three families serves to minimize the opportunities for common systematic faults, concurrent execution profiles, and similar responses to external influences that can contribute to the potential for CCF vulnerabilities in digital I&C systems.

Table 3 provides an overview of the three baseline strategies in terms of criteria adapted from NUREG/CR-6303. The basis for the strategy classifications was the technology employed, given that this fundamental difference between systems provides an identifiable, easily recognizable diversity characteristic of system design. Acceptable variants of these three strategies were also developed.

Table 3. Overview of baseline diversity strategies

Diversity attribute	Strategy[a]		
	A	B	C
Design			
Different technologies	x	–	–
Different approach—same technology	–	x	–
Different architectures	i	i	x
Equipment Manufacturer			
Different manufacturer—different design	x	x	–
Same manufacturer—different design	–	–	–
Different manufacturer—same design	–	–	x
Same manufacturer—different version	–	–	–
Logic Processing Equipment			
Different logic-processing architecture	i	i	x
Different logic-processing versions in same architecture	–	–	–
Different component integration architecture	i	x	x
Different data-flow architecture	i	–	–
Functional			
Different underlying mechanisms	i	i	–
Different purpose, function, control logic, or actuation means	x	x	x
Different response-time scale	–	–	–
Life Cycle			
Different design organizations/companies	x	x	x
Different management teams within same company	–	–	–
Different design/development teams (designers, engineers, programmers)	i	i	i
Different implementation/validation teams (testers, installers, or certification personnel)	i	i	i
Logic			
Different algorithms, logic, and program architecture	i	x	x
Different timing or order of execution	i	i	–
Different runtime environment	i	i	x
Different functional representation	i	i	x
Signal			
Different parameters sensed by different physical effects	x	x	x
Different parameters sensed by same physical effects	x	x	x
Same parameter sensed by different redundant set of similar sensors	x	x	x

[a]Intentional diversity (x), inherent diversity (i), not applicable (–).

DESIGN EVALUATION APPROACH

The grouping of diversity combinations according to Strategies A, B, and C facilitates a systematic organization of strategies into families that are readily amenable to evaluate. The classification of strategies enables a consistent representation of the comparative use of diversity between systems, redundancies, subsystems, modules, or components. As a consequence, this research leads to a systematic evaluation process for reviewing the application of diversity strategies to address CCF vulnerabilities identified through a D3 assessment.

The principal elements of the diversity evaluation process, which is applicable to confirm the response to any CCF vulnerabilities identified via a D3 assessment, include the following steps.

1. Classify the diversity strategy—identify what technology is employed.
2. Confirm inherent diversity credit—ensure that intrinsic benefits of technology differences are not compromised.
3. Identify intentional diversity usage—verify which intentional diversities are explicitly employed to address CCF.
4. Categorize diversity usage as a function of one of the following:
   - Strategy A, B, or C;
   - one of the variants of A, B, or C; or
   - alternate strategy.
5. Assess the diversity strategy—The diversity usage tables (as illustrated in Table 3) and a diversity assessment tool (see Appendix A of NUREG/CR-7007), which were developed through this research, provide support for comparative evaluations against the baseline diversity strategies.
6. Determine if the diversity strategy is adequate—A conclusion that a proposed diversity strategy adequately addresses CCF mitigation needs, as identified via a D3 assessment, can be based upon either conformance to one of the three baseline strategies (or an accepted variant) or determination that the strategy reasonably ensures CCF mitigation comparable to that provided by a baseline strategy (i.e., an acceptable rationale is provided to support mitigation claims).

The evaluation process for diversity strategies is intended to appropriately credit the inherent diversities arising from the chosen technologies while emphasizing identification of the intentional diversities explicitly employed to address the potential CCF vulnerabilities. In assessing the rationale for an alternate diversity strategy, the impact of each diversity criteria on purpose, process, product, and performance aspects of the diverse systems should be considered. The objective is to confirm that the diversity strategy provides sufficient CCF mitigation capability by adequately minimizing the opportunity for common systematic faults, reducing the occurrence of concurrent execution profiles, and lessening the likelihood of similar responses to external influences.

CONCLUSIONS

The results of this research effort have identified and developed diversity strategies, which consist of combinations of diversity attributes and their associated criteria, by leveraging the experience and practices of nonnuclear industries and the international nuclear power community. Effectively, these baseline sets of diversity criteria constitute appropriate mitigating strategies that adequately address potential CCF vulnerabilities in digital safety systems. The strategies represent guidance on acceptable diversity usage and can be applied directly to ensure that CCF vulnerabilities identified via a D3 assessment have been adequately resolved. Alternately, the strategies can serve as comparative norms, in combination with the diversity usage tables and/or diversity assessment tool developed in this research, to support confirmation that equivalent CCF mitigation capability is provided.

ACKNOWLEDGMENTS

This paper provides an account of work conducted under the sponsorship of the U.S. Nuclear Regulatory Commission. The opinions and conclusions of the authors expressed herein do not necessarily state or reflect those of the U.S. Nuclear Regulatory Commission or the Oak Ridge National Laboratory.

REFERENCES

Center for Chemical Process Safety, *Guidelines for Safe Automation of Chemical Processes*, American Institute of Chemical Engineers, New York, New York (1993).

International Atomic Energy Agency, *Radiation Aspects of Design for Nuclear Power Plants*, IAEA S-G-1.3, Vienna, Austria (2005).

International Electrotechnical Commission, “Instrumentation and Control Systems Important to Safety—Requirements to Cope with Common Cause Failure (CCF),” IEC 62340, Geneva, Switzerland (2008).

International Electrotechnical Commission, “Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Software Aspects for Computer-Based Systems Performing Category A Functions,” IEC 60880, Ed. 2.0, Geneva, Switzerland (2006).

U.S. Code of Federal Regulations, Title 10, Part 50, “Domestic Licensing of Production and Utilization Facilities,” Washington, DC (2004).

U.S. Nuclear Regulatory Commission, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Branch Technical Position 7-19, Washington, DC (2007).

U.S. Nuclear Regulatory Commission, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, “Instrumentation and Controls,” NUREG-0800, Chapter 7, Rev.5, Washington, DC (2007).

U.S. Nuclear Regulatory Commission, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, Washington, DC (1994).

U.S. Nuclear Regulatory Commission, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, NUREG/CR-7007, Washington, DC (2009).