Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies
NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2010)

DIVERSITY STRATEGIES TO MITIGATE POSTULATED COMMON CAUSE FAILURE VULNERABILITIES

Richard T. Wood
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831-6010
woodrt@ornl.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 (I&C) 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.

Key Words: *I&C, digital, diversity, nuclear power, common-cause failure*

1 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 (BTP) 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems" [1], within Chapter 7, "Instrumentation and Controls," of NUREG-0800, *Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants* [2]. 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 (ORNL) 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.

1.1 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 (DBAs) 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, as well as 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 (RTS), 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) [3], establish the minimum design requirements for light-water reactors (LWRs). 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* [4]. 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.

1.2 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 (FAA), the Center for Chemical Process Safety (CCPS) and the Federal Railway Administration (FRA). 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 the I&C systems at international evolutionary nuclear power plants (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, Temelin 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 applications. 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, application-specific integrated circuits, and multi-aperture magnetic ladder-like logic structures (Laddic) required revisions to the diversity attributes to assure 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.

2 NATURE OF CCF

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" [5]. 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" [6]. 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" [7].

3 USAGE OF DIVERSITY

The study of diversity in nonnuclear industries identified different approaches that range 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). The primary diversities cited for establishing sufficient application independence are functional, signal, software, and life-cycle (associated with the application software). While some examples of diversity usage have been noted in other industries, there has been little explicit guidance and infrequent dependence on this approach. 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.

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 digital I&C system architectures 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.

4 IMPACT OF DIVERSITY

The need for diversity within the I&C system architecture of an NPP is determined through conduct of a D3 analysis, such as the method established in NUREG/CR-6303. Where it is concluded that diversity is necessary to adequately address CCF vulnerabilities associated with a safety function, an

automatic diverse means for accomplishing the same safety function or an equivalent compensating function may be provided. Within the nuclear power industry, implementation of diversity to mitigate the effect of a potential CCF on safety functions is typically provided either through diverse elements (e.g., redundancies, subsystems, components) within the safety system or a separate diverse system (e.g., ATWS or diverse actuation system [DAS]). Essentially, the architectural approach in which diversity is normally employed can be represented in terms of two or more parallel diverse systems whose collective action in response to detection of an event reflects a one-out-of-two (or N) relationship (i.e., effectively providing a simple logical "OR"). The functionality embodied in these diverse systems is generally similar in nature (i.e., functional processing of measured data reflecting the plant condition leading to initiation of compensatory action when safety limits are challenged), although they may vary in purpose (i.e., control, limitation, or protection), approach (e.g., continuous control, one-time initiation, on-demand discrete manipulation), or functional relationships (e.g., different initiation criteria for the same event).

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 are based on characterization of diversity effects in terms of impact on common systematic faults, concurrent execution profiles, or similar responses to external influences.

5 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., 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 I 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 I. 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 a different redundant set of similar sensors	x	x	x

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

6 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 I) and a diversity assessment tool (see Reference 8), 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.

7 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.

8 ACKNOWLEDGMENTS

The author gratefully acknowledges the guidance and assistance provided by Michael E. Waterman of the U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research during the course of the research described in this paper. The author would like to recognize the many staff members of Oak Ridge National Laboratory who contributed technical insight and expertise to the project. This paper provides an account of work conducted under the sponsorship of by the U.S. Nuclear Regulatory Commission. The opinions and conclusions of the author expressed herein do not necessarily state or reflect those of the U.S. Nuclear Regulatory Commission or the Oak Ridge National Laboratory.

9 REFERENCES

1. 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).
2. 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).
3. *U.S. Code of Federal Regulations*, Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.
4. U.S. Nuclear Regulatory Commission, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, Washington, DC (1994).
5. International Atomic Energy Agency, "Radiation Aspects of Design for Nuclear Power Plants," IAEA S-G-1.3, Vienna, Austria (2005).
6. International Electrotechnical Commission, "Instrumentation and Control Systems Important to Safety—Requirements to Cope with Common Cause Failure (CCF)," IEC 62340, Geneva, Switzerland (2008).
7. 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).
8. U.S. Nuclear Regulatory Commission, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, NUREG/CR-7007, Washington, DC (2008).